AUDITORÍA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. DEL DEPARTAMENTO DE NARIÑO

LAURA YANETH NOGUERA QUENGUAN
EDY YANIRA SANCHEZ PERENGUEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2012

AUDITORÍA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. DEL DEPARTAMENTO DE NARIÑO

LAURA YANETH NOGUERA QUENGUAN
EDY YANIRA SANCHEZ PERENGUEZ

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

Director
ING. MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2012

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva del autor.

Artículo 1ro del Acuerdo No. 324 de octubre 11 de 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

NOTA DE ACEPTACIÒN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 2012

AGRADECIMIENTOS

A ti Señor el más especial agradecimiento, por darnos la oportunidad de culminar nuestros estudios con valor y fortaleza en el transcurso de nuestra carrera.

Con mucho cariño a nuestros Padres por el esfuerzo y apoyo incondicional que nos brindaron día a día, por compartir inolvidables momentos de nuestras vidas, gracias por ayudarnos a cumplir nuestros sueños, por darnos la oportunidad de formarnos como profesionales.

Al Ingeniero Manuel Bolaños, por su apoyo y compromiso en el desarrollo y culminación de este trabajo.

Al Ingeniero Francisco Nicolás Solarte, por su apoyo y acompañamiento, por su dedicación, por transmitir sus conocimientos y su experiencia profesional en el desarrollo de este trabajo.

Al Ingeniero Harold Caicedo, Jefe del área de Sistemas de Emssanar E.S.S Nariño, por darnos la oportunidad de aplicar y ampliar nuestros conocimientos en esta Empresa y por la confianza, apoyo y colaboración prestada durante el desarrollo de este trabajo.

A nuestros Maestros y Amigos, mil gracias porque de alguna manera forman parte de lo que ahora somos, por las enseñanzas, confianza, amistad, tiempo y apoyo sincero dedicado durante la trayectoria de aprendizaje y conocimiento.

DEDICATORIA

A Dios por darme la bendición y oportunidad de vivir y recorrer este camino, por darme la fortaleza de seguir adelante en los momentos difíciles.

A mis padres fuente de mi inspiración, por su gran esfuerzo y dedicación para culminar mis estudios, en especial a mi Padre que repentinamente emprendió un viaje sin regreso y a quien dedico este logro como símbolo de todo el agradecimiento a su amor, confianza, motivación, empeño y apoyo incondicional para seguir adelante**,** a mis hermanos y en si a toda mi familia por sus consejos y palabra de aliento por formar parte de mí, por todo lo que me han brindado y por sus bendiciones.

Laura Yaneth Noguera Quenguan

Dedico este trabajo a Dios, por su bendición constante en mi vida y en mi carrera profesional, por ser esa fuerza interna que me ayudo en los momentos difíciles para seguir adelante y poder culminar mi trabajo.

A mis padres por el esfuerzo, la dedicación, el sacrificio, el apoyo y la motivación durante todo este tiempo, porque ellos son la razón por la cual todos los días encamino mis esfuerzos para salir adelante y ser una mejor persona.

A toda mi familia por creer en mí y por brindarme la confianza y el apoyo necesario a lo largo de mi carrera, por su cariño incondicional y por ser parte de mi vida.

Edy Yanira Sánchez Perenguez

RESUMEN

LA AUDITORÍA APLICADA A LAS DIFERENTES ÁREAS DE UNA DETERMINADA EMPRESA SE HA CONVERTIDO EN LA ACTUALIDAD EN UNA NECESIDAD URGENTE PARA EL DESARROLLO Y CRECIMIENTO EMPRESARIAL YA QUE A TRAVÉS DE LA REVISIÓN Y EVALUACIÓN DE LAS DIFERENTES ÁREAS PERMITE EVALUAR LA EFICIENCIA Y EFICACIA DE CADA UNO DE LOS PROCESOS**.**

LA NECESIDAD DE EVALUAR LOS PROCESOS DEL ÁREA DE SISTEMAS DE LA ENTIDAD DE SALUD EMSSANAR E.S.S SURGE A TRAVÉS DE LA BÚSQUEDA CONTINUA DE MEJORAMIENTO, EMPRENDIMIENTO Y CRECIMIENTO EMPRESARIAL, TENIENDO COMO OBJETIVO PRIMORDIAL MEJORAR CONTINUAMENTE LA CALIDAD DE ATENCIÓN Y PRESTACIÓN DE SERVICIO DE SALUD AL USUARIO.

LA AUDITORIA INFORMÁTICA EN EL ÁREA DE SISTEMAS DE EMSSANAR E.S.S SE REALIZA CON EL FIN DE EVALUAR LA EFICIENCIA Y EFICACIA DEL HARDWARE DE COMUNICACIONES, LOS SERVIDORES E INDICADORES DE FUNCIONAMIENTO, TENIENDO EN CUENTA QUE LA ADMINISTRACIÓN DE LOS RECURSOS TIC ES FACTOR CLAVE PARA EL DESEMPEÑO Y FUNCIONAMIENTO DE LAS DIFERENTES ACTIVIDADES QUE SE DESARROLLAN DENTRO DE LOS PROCESOS PERTENECIENTES A ESTA ÁREA, IDENTIFICANDO VULNERABILIDADES QUE PERMITAN OBTENER UN DIAGNOSTICO PARA QUE POR MEDIO DE ESTE LA ENTIDAD DEFINA PLANES DE MEJORAMIENTO A NIVEL DE PROCESOS Y POR ENDE A NIVEL EMPRESARIAL.

PARA EL DESARROLLO DE LA AUDITORIA SE TOMA COMO PUNTO DE REFERENCIA EL MODELO COBIT (OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN), SELECCIONANDO Y APLICANDO LOS PROCESOS DE CADA DOMINIO RELATIVO A LOS OBJETIVOS DE LA AUDITORIA.

ABSTRACT

THE AUDIT APPLIED TO DIFFERENT AREAS OF A PARTICULAR COMPANY HAS NOW BECOME AN URGENT NEED FOR THE DEVELOPMENT AND FOR THE BUSINESS GROWTH, SINCE THROUGH THE REVIEW AND EVALUATION OF THE DIFFERENT AREAS IT IS ALLOWED TO ASSESS THE EFFICIENCY AND EFFECTIVENESS OF EACH THE PROCESSES.

THE NEED TO EVALUATE THE PROCESSES OF THE SYSTEMS AREA FROM THE ESS EMSSANAR HEALTH ENTITY EMERGES THROUGH THE STEADY SEARCH FOR IMPROVEMENT, ENTREPRENEURSHIP AND BUSINESS GROWTH, HAVING AS THE PRIMARY AIM TO CONTINUALLY IMPROVE THE QUALITY OF CARE AND PROVISION OF THE HEALTH SERVICE ITSELF TO THE VERY USERS.

COMPUTER AUDIT IN THE SYSTEMS AREA FROM EMSSANAR ESS IS CARRIED OUT TO ASSESS THE EFFICIENCY AND EFFECTIVENESS OF THE COMMUNICATIONS' HARDWARE, THE SERVERS AND THE PERFORMANCE INDICATORS, TAKING INTO ACCOUNT THAT THE MANAGEMENT OF THE TIC RESOURCES IS THE KEY FACTOR FOR THE PERFORMANCE AND THE OPERATION OF SEVERAL ACTIVITIES DEVELOPED WITHIN THE PROCESSES WHICH BELONG TO THIS AREA BY IDENTIFYING VULNERABILITIES THAT ALLOW A DIAGNOSIS PROCESS SO AS TO THROUGH ITSELF, THE ENTITY DEFINES IMPROVEMENT PLANS AT PROCESSES LEVEL AND THUS AT ENTERPRISE LEVEL.

FORT THE DEVELOPMENT OF THE AUDIT, IT IS TAKEN AS A REFERENCE POINT THE COBIT MODEL (CONTROL OBJECTIVES FOR THE INFORMATION TECHNOLOGY), BY SELECTING AND APPLYING THE PROCESSES OF EACH OF THE DOMAINS RELATED TO THE AIMS OF THE AUDIT.

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

GLOSARIO

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Backup: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables problemas si se realiza de forma habitual y periódica.

Centro de cómputo: Es un área de trabajo cuya función es la de concentrar, almacenar y procesar los datos y funciones operativas de una empresa de manera sistematizada.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Cliente: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

COBIT: (Control Objetives for Information and related Technology) Objetivos de Control para la información y tecnología relacionadas. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control

de tecnología de información, aceptados para ser empleados por gerentes de empresas y auditores.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datos: Término general para la información procesada por un ordenador.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Dominio: Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión de TI.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según
[ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.

Información: En sentido general, es todo lo que reduce la incertidumbre y sirve para realizar acciones y tomar decisiones.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

Internet: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: (Information Systems Audit and Control Association) Asociación de Auditoría y Control de los Sistemas de Información. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISO: (International Organization for Standardization) Organización Internacional para la Normalización. Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

Mantenimiento Correctivo: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad, con el fin de prevenir su repetición.

Mantenimiento Preventivo: Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Organización: Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones. Una organización puede ser pública o privada.

Políticas de seguridad: Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, rol claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Red: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Riesgo: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Seguridad de la información: Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

TI: Tecnologías de Información

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

Actualmente la tecnología juega un papel fundamental en el mantenimiento de las empresas, es la base de comportamiento de cada empresa, a nivel de organización y desarrollo; el proveer a cualquier empresa de tecnología es hoy en día una necesidad primordial, ya que la sistematización trae como resultado la mejora del cumplimiento de los objetivos empresariales. Teniendo en cuenta la falta de organización, daños o pérdidas financieras o administrativas se hace necesario definir métodos y controles que ayuden a estimar la magnitud del manejo de cada área o de cada proceso que se lleve dentro de la empresa como tal. Todo esto lo aplica la auditoria con el objetivo de evaluar a través de la aplicación de diferentes técnicas que garanticen la confidencialidad, integridad y disponibilidad de la información de todos los procesos que formen parte de la empresa.

Una empresa debe estar en continua evaluación para mirar sus falencias y tomar acciones que mejoren la eficiencia y eficacia en sus procesos y así ubicarse dentro de un medio competitivo, para ello se han creado diferentes métodos encaminados a buscar este objetivo. Uno de los principales es la auditoría informática, factor importante para el buen desempeño de una empresa, ya que proporciona los controles necesarios para que la información y los procesos sean confiables, entregando un diagnóstico de cómo está la empresa en una determinada área y a la vez permita crear un plan de mejoramiento mediante las recomendaciones dadas.

Emssanar es una Empresa Solidaria de Salud del Régimen Subsidiado que integra a mas de 1’200.000 afiliados en el sur occidente colombiano; cuenta con una red de 370 IPS en los departamentos de Nariño, Putumayo, Cauca y Valle, integradas a través de un innovador Centro de Contactos que permite mejorar la atención al usuario. Emssanar siempre se ha preocupado por mantenerse en los primeros lugares en cuanto a prestación de servicios de salud se refiere, enfocando sus objetivos al mejoramiento de todos los procesos, como lo es el área de sistemas quien es la encargada de la administración de los sistemas operativos con el objetivo de garantizar la continuidad y el funcionamiento de las maquinas y del software al máximo rendimiento.

Teniendo en cuenta que el activo más importante de una organización es la información, por ende los recursos tecnológicos que utilizan y que en ellos se registra y procesa la información, hay que tener en cuenta que también son susceptibles de amenazas, por ello se hace necesario contar con planes y políticas para proteger estos recursos, por tal razón se presenta el trabajo de grado **AUDITORIA INFORMATICA EN EL AREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. DEL DEPARTAMENTO DE NARIÑO,** el cual corresponde a la modalidad de trabajo de aplicación bajo la línea de investigación de Sistemas Computacionales.

La aplicación de esta auditoría va encaminada a evaluar la parte física del área de sistemas en los procesos de comunicaciones, servidores del hardware e indicadores de

funcionamiento dentro de los cuales se evaluara el cumplimiento de los niveles de cobertura, de obsolescencia, de soporte Tecnológico, de Riesgo y Tiempo fuera de servicio, con el fin de identificar algunas vulnerabilidades a los que estén expuestos estos procesos y que el objetivo es mejorar para obtener un funcionamiento del área de sistemas que permita solidificar procesos de calidad.

El presente documento está organizado así: en la primera parte se plantea el tema del proyecto, el cual se encuentra dentro de una de las líneas de investigación aprobadas por el departamento de sistemas, seguido de la descripción del problema, de los objetivos que se pretende alcanzar, como también se tiene en cuenta los antecedentes tomados como base para iniciar la recolección de información, la factibilidad del proyecto y la metodología a seguir y el desarrollo de la auditoría como tal, donde se encuentra el archivo permanente que contiene información del área donde se va a realizar la auditoria, seguido del archivo corriente que contiene las herramientas necesarias para la recolección de información para la ejecución de la auditoria, luego se describen los hallazgos encontrados, seguido del informe general e informe ejecutivo donde se describen los riesgos encontrados con sus respectivas recomendaciones, finalmente se encontraron algunas sugerencias y recomendaciones que se hacen a la empresa auditada con el fin de implementar un plan de mejoramiento que garantice fortalecer las debilidades encontradas.

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S DEL DEPARTAMENTO DE NARIÑO.

TEMA

Auditoria aplicada al área de sistemas, en la parte de hardware e indicadores de funcionamiento de la Empresa Solidaria de Salud Emssanar E.S.S. de Nariño.

MODALIDAD

Este trabajo de grado, corresponde a la modalidad de TRABAJO DE APLICACION, a realizarse en la **EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.** Trabajo que permitirá ampliar conocimiento y generar diferentes alternativas de desarrollo empresarial a través de la aplicación de métodos de organización, funcionamiento y aplicación y cumplimiento de políticas, leyes y normas, necesarios para el funcionamiento de una empresa.

LINEA DE INVESTIGACION

Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de facultad 045 de octubre 10 de 2002 dado por el consejo de facultad, el proyecto corresponde a la línea de investigación de Sistemas Computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de auditoría de sistemas.

DEFINICION DEL PROBLEMA

Planteamiento del Problema. Los procesos de continua evaluación son importantes en una empresa ya que de estos se desglosan los posibles problemas que afectan a la empresa, teniendo en cuenta estos se crean medidas que contrarresten estas debilidades.

Actualmente en Emssanar E.S.S no se ha revisado ni evaluado la eficiencia y eficacia del área de sistemas en la parte física de comunicaciones, servidores e indicadores,

información valiosa para la empresa ya que si el proceso de las comunicaciones y todo lo que tiene que ver con ella no es el adecuado, la empresa puede enfrentar problemas que afectan el funcionamiento y desempeño de todos los procesos de los cuales depende el área de sistemas.

Con lo anterior y teniendo en cuenta que para lograr un buen desempeño debe existir en la empresa una buena organización y estructuración de la misma como tal y conociendo el tiempo de funcionamiento que lleva la empresa y que hasta ahora no se ha llevado a cabo una auditoria de este tipo se hace indispensable revisar el control, la administración y mantenimiento del hardware de los equipos de comunicación, los servidores e indicadores de funcionamiento que hacen parte del área de sistemas de esta entidad.

En Emssanar E.S.S, se realizará una auditoría que permita obtener un diagnóstico como resultado de la identificación de riesgos y hallazgos, analizarlos para así hacer las respectivas recomendaciones que permitirán a la empresa desarrollar un plan de mejoramiento que conlleve a una buena toma de decisiones y así mismo a optimizar sus procesos.

Formulación del problema. ¿Cómo evaluar la eficiencia y eficacia del hardware de las comunicaciones, los servidores e indicadores de funcionamiento en el área de sistemas de Emssanar E.S.S?

Sistematización del problema.

- ¿Cómo identificar los posibles puntos críticos dentro de los procesos del hardware del área de sistemas en cuanto a comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento de la empresa?

- ¿Cómo realizar el proceso de auditoría aplicando estándares que permita revisar y evaluar los 4 campos tomados como caso de estudio de la empresa dentro del departamento de Nariño?

- ¿Cómo identificar falencias y puntos críticos en la parte de comunicaciones en cuanto a proveedores, contratos y soporte?

- ¿Cómo identificar falencias y puntos críticos en aseguramiento eléctrico y físico de los equipos de cómputo y de los equipos de comunicaciones?

- ¿Cómo identificar falencias y puntos críticos en los servidores en cuanto a garantías, instalaciones, respaldos, planes de contingencia, políticas de seguridad y política de mantenimiento?

- ¿Cómo verificar que se cumplan los indicadores en los niveles de cobertura, de obsolescencia, de soporte Tecnológico y Tiempo fuera de servicio?

OBJETIVOS

Objetivo general. Evaluar la eficiencia y eficacia del hardware de las comunicaciones, los servidores e indicadores de funcionamiento en el área de sistemas de Emssanar E.S.S, obteniendo un diagnostico que permita definir planes de mejoramiento en la empresa Solidaria de Salud Emssanar E.S.S.

Objetivos específicos

- ✓ Identificar cada uno de los procesos y procedimientos correspondientes al hardware de las comunicaciones, servidores, equipos de cómputo e indicadores del área de sistemas de la Empresa EMSSANAR E.S.S.

- ✓ Identificar debilidades y fortalezas en la parte física de las comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento.

- ✓ Identificar cada uno de los 4 campos tomados como caso de estudio y proceder a realizar la auditoria en cada uno de ellos.

- ✓ Identificar el funcionamiento de las comunicaciones en cuanto a proveedores, contratos y soporte.

- ✓ Identificar el funcionamiento de los servidores en cuanto a garantías, instalaciones, respaldos, políticas de contingencia, políticas de seguridad y políticas de mantenimiento.

- ✓ Verificar el cumplimiento de los indicadores de funcionamiento en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio.

JUSTIFICACIÓN

La auditoria debe estar encaminada a un objetivo específico que es el de evaluar 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, que lleve a la empresa auditada a cumplir con las normas de calidad establecidas.

Como se expuso anteriormente, en Emssanar E.S.S no se ha revisado ni evaluado el hardware en el área de sistemas en comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento, información que es importante para la empresa y con la cual no cuenta actualmente, por ese motivo se ha planeado realizar un proceso de auditoría que solvente esta necesidad.

Este proyecto va encaminado a solventar estas necesidades y para ello se realizará una auditoría donde se obtendrá un plan de mejoramiento que ayudara a la empresa a

identificar cuáles son los niveles de riesgo, puntos fuertes, puntos débiles, oportunidades y amenazas en los 4 campos tomados como caso de estudio (regional Nariño, principal Pasto, zonal Ipiales y municipal Córdoba); mediante la aplicación del modelo COBIT en los diferentes procesos de la auditoría, la empresa podrá asegurar la calidad en el área de sistemas obteniendo un diagnóstico que permita generar un plan estratégico que asegure el manejo y control de la información concernientes al hardware de las comunicaciones, de servidores, de equipos de computo e indicadores de funcionamiento.

ALCANCE Y DELIMITACIÓN

Conociendo que Emssanar cubre los departamentos de Valle, Cauca, Putumayo y Nariño, la auditoria se realizó únicamente en el departamento de Nariño, por lo tanto el trabajo se aplicó a 4 campos tomados como caso de estudio en la empresa, clasificados así:

- *Regional => Nariño*
- *Central => Pasto*
- *Zonal => Ipiales*
- *Municipal => Córdoba*

Durante el desarrollo del proyecto se identificaron las técnicas y el modelo de auditoría informática que se aplicó al área de sistemas de Emssanar E.S.S, donde se realizó un diagnóstico permitiendo revisar y evaluar procesos mediante el uso de normas y estándares internacionales de calidad como es el modelo COBIT, logrando así identificar diferentes vulnerabilidades en el manejo y mantenimiento aplicado a la parte física de:

- **Comunicaciones:** verificar proveedores, soporte, contratos, aseguramiento eléctrico y físico de los equipo de comunicaciones.
- **Servidores:** revisar garantías, instalaciones, respaldos, planes de contingencia, políticas de seguridad, política de mantenimiento con sus respectivos formatos de registro e instructivos.
- **Equipos de Computo:** revisar garantías, instalaciones, respaldos, planes de contingencia, políticas de seguridad, política de mantenimiento con sus respectivos formatos de registro e instructivos.
- **Indicadores de funcionamiento:** verificar el cumplimiento de los niveles de cobertura, de obsolescencia, de soporte Tecnológico y Tiempo fuera de servicio.

Logrando que la entidad mediante los resultados obtenidos desarrolle un plan de mejoramiento que le permita tomar medidas de seguridad y control de la parte física en cuanto a comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento del área de sistemas.

1. MARCO TEORICO

1.1. ANTECEDENTES

La naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevarse a cabo, requieren el desarrollo y la promulgación de normas generales para la auditoría de los sistemas de información. La auditoría de los sistemas de información se define como la revisión y evaluación de todos los aspectos, de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo.

Razón que conlleva a que en la actualidad se han presentado cambios en el enfoque tradicional de las Auditorías sometiéndolas a procesos de reingeniería acorde a la evolución tecnológica, donde la misma genere valor agregado a través de su enfoque preventivo intentando actuar antes o después del hecho. El incremento masivo en el uso de las computadoras y el desarrollo de aplicaciones cada vez más sofisticadas han instado la necesidad de adoptar diferentes técnicas de auditoría para hacer frente a estos cambios. Planteadas entonces las nuevas exigencias del Control Interno y teniendo en cuenta los modelos de control existentes tales como COSO, COCO, etc., se plantea el empleo de un nuevo modelo llamado COBIT cuyas siglas significan: Objetivos de Control para la información y tecnologías afines.

El Modelo COBIT supone un enfoque distinto y actual del sistema por cuanto lo mira en su ámbito global, formado por procesos manuales y automatizados. El Modelo COBIT supone un aporte de máximo interés para los auditores ya que incorpora aspectos de gestión de la calidad total, reingeniería de empresas e integra los dos modelos de control: los orientados a las tecnologías de información y los orientados a los objetivos empresariales.

La evaluación de los requerimientos del negocio, los recursos y procesos IT (información y tecnología), son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y la tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.
La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Existen diferentes tipos de auditorías que en la Universidad de Nariño, en el programa de Ingeniería de Sistemas se han realizado, entre ellas:

TÉCNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PÁGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO, realizada por Liliana Caicedo Mora y Claudia Ordoñez Burbano, este trabajo consistió en Aplicar técnicas de auditoría de sistemas a entidades públicas del Departamento de Nariño para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación (TI), y el cumplimiento del Decreto 1151 sobre Gobierno en Línea.

AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO, realizada por Oscar Julián Estrada Obando, este trabajo consistió en realizar la evaluación de los controles relacionados con la seguridad física de la información, realizar la evaluación de los controles relacionados con la seguridad lógica de la información, Identificar las fallas en cuestión de seguridad, plantear posibles soluciones para mejorar las condiciones de seguridad físicas y lógicas del Sistema Integral de Información.

AUDITORIA MODULO DE HISTORIA CLÍNICA ELECTRÓNICA DEL SISTEMA DE INFORMACIÓN EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO, realizado por Jenny Burgos García y Carolina Domínguez, este trabajo consistió en la revisión de controles existentes en cuanto al cumplimiento de los diferentes requerimientos de los usuarios del módulo de historia clínica y la seguridad lógica de del sistema operativo y acceso a la base de datos.

1.2. ASPECTOS GENERALES DE LA AUDITORIA

Uno de los avances más importante de los últimos años es la tecnología y con ello el cambio drástico que el mundo ha tenido con el paso del tiempo, el competitivo campo laboral ha adaptado de forma muy positiva el manejo de la tecnología, teniendo como resultado que la información de una empresa este bien organizada, de esta manera se hace necesario tener un control de las herramientas como equipos de computo, equipos de comunicación, bases de datos, redes y sistemas de información, para saber así con que herramientas se cuenta y que tan actualizados están, lo anterior combinado con la necesidad de obtener un plan estratégico y corporativo que le permita a la empresa conocer las fortalezas y debilidades que genere a la parte administrativa seguridad, confiabilidad, efectividad y eficacia de su entorno, a partir de esto se hace necesario que se lleve a cabo una auditoria de acuerdo a las necesidades que existan en la empresa.

Por lo general, el área de sistemas de una empresa, es un espacio dotado de recursos tecnológicos como equipos de cómputo, impresoras, equipos de comunicaciones, donde prácticamente se realiza todo el procesamiento de la información, que por razones de

organización se hace necesaria la auditoría Existen algunas funciones del área de sistemas, que son:

Administración de sistemas y soporte centralizados[1]*.* Gran parte de la actividad que se desarrolla en el área de sistemas corresponde a la administración de los sistemas operativos y al soporte a los usuarios de los computadores centrales o corporativos, con los objetivos de garantizar la continuidad del funcionamiento de las máquinas y del software al máximo rendimiento, y facilitar su utilización a todos los sectores de la comunidad de la empresa. Se desarrollan las siguientes tareas:

- Mantenimiento de los equipos.
- Sintonía del sistema operativo y optimización del rendimiento.
- Gestión de cuentas de usuario y asignación de recursos a las mismas.
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.
- Evaluación de necesidades de recursos (memoria, discos, unidad central) y provisión de los mismos en su caso.
- Instalación y actualización de utilidades de software.
- Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento, etc).
- Organización de otros servicios como copia de ficheros (Backus), impresión desde otros ordenadores en impresoras dependientes de estos equipos.

Funciones del área de sistemas y comunicaciones[2]*.* La misión fundamental del área, es el diseño, implementación y mantenimiento de los elementos que constituyen la infraestructura informática de la empresa, como los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la comunidad los servicios informáticos necesarios para desarrollar sus actividades. Como también se encarga de:

- La red informática, de los ordenadores centrales que están a disposición de los usuarios y/o que prestan servicios a los ordenadores personales, así como de las aplicaciones instaladas en ellos y los servicios de uso general, como por ejemplo el correo electrónico.
- Instalación y configuración de los ordenadores centrales.
- Altas y bajas de usuarios.
- Instalación y configuración de aplicaciones en los servidores.
- Mantenimiento de los discos de usuarios.
- Administración de las listas de correo.
- Copias de seguridad de los datos de los usuarios y recuperación de los mismos en caso de pérdida.
- Instalación, configuración y mantenimiento de servicios como correo electrónico, proxy Web, FTP anónimo.
- Diseño y configuración de la red.

[1] http://benmp82.galeon.com/funsis.htm
[2] http://benmp82.galeon.com/funsis.htm

Existen diferentes tipos de auditoría que se aplican de acuerdo a la necesidad, donde se busca encontrar y evaluar diferentes procesos y evidencias. Generalmente es realizada por una persona independiente y competente acerca de la información que se maneja en una empresa de igual manera detecta los puntos exactos de control en las distintas dependencias, permitiendo[3]:

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática, las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los sistemas de información.

La auditoria informática es la evaluación de los recursos tecnológicos, deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, según sea la necesidad planteada en el proyecto, además es importante para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

1.2.1 Definición de auditoría. Auditoria es un examen complejo que se realiza a una empresa, evaluando cumplimiento de normas, proyectos, la parte financiera, el cumplimiento de objetivos, en general evalúa la eficiencia y eficacia de todos los procesos que tienen que ver con el mejoramiento y desarrollo empresarial, determinando diferentes alternativas de soluciones para garantizar organización y logro de objetivos.

La eficiencia, definida como lograr el objetivo en menor tiempo posible y la eficacia definida como lograr el objetivo sin importar el tiempo, se convierte en la clave para obtener una auditoria de calidad.

Un auditor debe ser una persona capaz de observar cada movimiento y comportamiento de los procesos, encaminado siempre al objetivo especifico, que es el de evaluar la eficacia y eficiencia de cada proceso tomado como caso de estudio, para que por medio del señalamiento de alternativas de acción, la empresa como tal tome decisiones que permita corregir hallazgos en caso de que sean encontrados, mejorando las funciones de cada proceso permitiendo así el cumplimiento de los objetivos propuestos por la empresa.

[3] Arens, Alvin A. Auditoria un Enfoque Integral. 6 Edición. Méjico: Prentice Hall, 1996.

Existen diferentes tipos de auditoría, así como normas y procedimientos específicos para la realización de auditorías contables, como también normas y procedimientos para la realización de auditoría en informática como parte de una profesión, además la auditoria debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

1.2.2 Objetivo general de la auditoría.[4] El objetivo de la auditoria consiste en apoyar a los miembros de la empresa (Directorio y las Gerencias) en el desempeño de sus actividades, que le permitan la buena y oportuna toma de decisiones. Para ello la auditoria les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

1.2.3. Funciones principales[5]

- Evaluar la gestión de la empresa, para emitir sugerencias orientadas a mejorar la gestión administrativa, y asegurar la vigencia de una estructura de control interno sólida y efectiva.
- Verificar el debido cumplimiento de las funciones y responsabilidades asignadas a cada funcionario de la empresa.
- Evaluar el logro de los objetivos y metas, fijadas en los planes y programas, trazados por la empresa.
- Identificar y comunicar a las autoridades competentes, las desviaciones importantes en la ejecución de las actividades, que impiden lograr los objetivos y las metas previamente establecidas; recomendar las medidas correctivas para subsanar dichas desviaciones y cumplir la finalidad para que fue creada la empresa.
- Garantizar la calidad de la información financiera, administrativa o de cualquier otro tipo, de modo que permita a todos los niveles jerárquicos, tomar decisiones acertadas sobre una base firme y segura.
- Establecer el grado en que la prestación de servicios ofrecidos a la colectividad, se han logrado en forma eficiente, efectiva y económica.
- Verificar el cumplimiento de las disposiciones legales, reglamentarias, contractuales y normativas aplicables.
- Ejercer revisión en forma preventiva a los egresos ejecutados por la empresa.
- Evaluar los procesos informáticos de la empresa.

1.2.4. Clasificación de la auditoría

Auditoría externa

La auditoría externa se caracteriza principalmente por quien la realiza, ya que debe ser un profesional totalmente independiente de la empresa, el cual después de examinar y evaluar el área de los sistemas de información genera una opinión veraz y creíble de los casos de estudio tomados, para luego presentarlos como resultados o hallazgos a la empresa u organización.

[4]. http://www.monografias.com/trabajos14/auditoria/auditoria.shtml
[5] . http://www.hondutel.hn/portal_transparencia/pdf/auditoriainterna-2.pdf

Auditoría interna

La auditoría interna es la evaluación exhaustiva y detallada de cada uno de los procesos llevados dentro de una empresa, se evalúan sistemas de información como también operaciones contables y financieras, evaluando siempre la eficiencia y eficacia de todos los procesos. Generalmente la empresa es quien asigna a un profesional calificado perteneciente a la misma con el objeto de utilizar diferentes técnicas que permitan realizar un examen, dando como resultado la detección de fallas a tiempo, para corregirlas y mejorar algunos procesos que así el informe de la auditoria final lo sugiera. Es importante aclarar que la información de la auditoria es manejada por la dirección ya que el objetivo es obtener sugerencias para el mejoramiento y cumplimiento de las normas, operaciones, funciones y responsabilidades del núcleo empresarial.

El que cada empresa realizara una auditoría interna ayudaría en gran medida al desarrollo de la misma, ya que al detectar problemas o fallas en cualquier proceso, permite a la dirección como tal conocer a fondo el objetivo de cada departamento y como deben funcionar estos, permite a la misma empresa como tal elaborar planes estratégicos, planes de contingencia, eliminar la redundancia de procesos, etc., permitiéndoles a través de la evaluación, identificar los puntos débiles de la misma para mejorarlos, ayudando a proteger los interés para el desarrollo y crecimiento empresarial.

1.2.4 Tipos de Auditoria

Auditoría fiscal[6]

Se define como la verificación racional de los registros contables y de la documentación, con el fin de determinar la exactitud e integridad de la contabilidad. La auditoría fiscal consiste en la investigación selectiva de las cuentas del balance, de las cuentas de resultados, de la documentación, registro y operaciones efectuadas por una empresa, tendientes a comprobar que las bases afectas a tributos se hayan determinado de acuerdo con las normas técnicas que regulas la contabilidad y cumpliendo con las disposiciones legales contenidas en el Código de Comercio, Código Orgánico Tributario, y demás leyes impositivas que corresponda aplicar.

Auditoría Financiera[7]

Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la situación financiera de la empresa, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoría, ya que el auditor hace su trabajo posterior a las operaciones de la empresa.

[6] . http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml

[7] . http://www.gerencie.com/auditoria-financiera.html

Auditoria operacional[8]

Es una revisión y evaluación parcial o total de las operaciones y procedimientos adoptados en una empresa, con la finalidad principal de auxiliar a la dirección a eliminar las deficiencias por medio de la recomendación de medidas correctivas. Comprende además de la financiera, el examen y evaluación de la planeación, organización, dirección y control interno administrativo; de la eficiencia, eficacia y economía con que se han empleado los recursos humanos, materiales y financieros; y de los resultados de las operaciones programadas para saber si se han logrado o no los objetivos propuestos.

Auditoria administrativa[9]

Es el revisar y evaluar si los métodos, sistemas y procedimientos que se siguen en todas las fases del proceso administrativo aseguran el cumplimiento con políticas, planes, programas, leyes y reglamentaciones que puedan tener un impacto significativo en operación de los reportes y asegurar que la organización los esté cumpliendo y respetando.

Es el examen metódico y ordenado de los objetivos de una empresa de su estructura orgánica y de la utilización del elemento humano a fin de informar los hechos investigados.

Su importancia radica en el hecho de que proporciona a los directivos de una organización un panorama sobre la forma como está siendo administrada por los diferentes niveles jerárquicos y operativos, señalando aciertos y desviaciones de aquellas áreas cuyos problemas administrativos detectados exigen una mayor o pronta atención.

Auditoria integral[10]

Auditoría integral es el examen crítico, sistemático y detallado de los sistemas de información financiero, de gestión y legal de una organización, realizado con independencia y utilizando técnicas específicas, con el propósito de emitir un informe profesional sobre la razonabilidad de la información financiera, la eficacia eficiencia y economicidad en el manejo de los recursos y el apego de las operaciones económicas a las normas contables, administrativas y legales que le son aplicables, para la toma de decisiones que permitan la mejora de la productividad de la misma.

Auditoria informática[11]

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

---

[8] . http://www.definicion.org/auditoria-operacional

[9] . http://www.gerencie.com/auditoria-financiera.html

[10] . http://members.tripod.com/~Guillermo_Cuellar_M/integral.html

[11]. http://www.mitecnologico.com/Main/ConceptosAuditoriaYAuditoriaInformatica

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

1.3 AUDITORIA INFORMÁTICA COMO OBJETO DE ESTUDIO

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. Los factores que pueden influir en una organización a través del control y la auditoría en informática, son:

- Necesidad de controlar el uso evolucionado de las computadoras.
- Controlar el uso de la computadora, que cada día se vuelve más importante y costosa.
- Altos costos que producen los errores en una organización.
- Abuzo en las computadoras.
- Posibilidad de pérdida de capacidades de procesamiento de datos.
- Posibilidad de decisiones incorrectas.
- Valor del hardware, software y personal.
- Necesidad de mantener la privacidad individual.
- Posibilidad de pérdida de información o de mal uso de la misma.
- Necesidad de mantener la privacidad de la organización.

La información es un factor importante y cada día cobra más valor para una empresa u organización para la continuidad de las operaciones, ya que la imagen de su ambiente depende de la situación actual, su desarrollo y competitividad dependen del ambiente pasado y futuro, ya que tomar una decisión incorrecta mediante datos erróneos proporcionados por los sistemas trae como consecuencia efectos significativos que afectan directamente a la organización.

1.3.1 Objetivo fundamental de la auditoría informática. La operatividad en una empresa es el punto más importante, es encargada de vigilar el funcionamiento de mínimos consistentes de la organización y las máquinas a nivel global como parcial. La auditoria se debe realizar en el momento en que la maquinaria informática está en funcionamiento, con el fin de identificar falencias que obstruyan la operatividad de las mismas, con el objeto de corregir o buscar alternativas de solución a tiempo, sin tener que parar el trabajo.

La operatividad de los sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

Los Controles Técnicos Generales son importantes en las instalaciones de empresas grandes, ya que se realizan para verificar la compatibilidad de funcionamiento simultáneo del sistema operativo y el software de base con todos los subsistemas existentes, como también la compatibilidad del hardware y del software instalado. En una empresa existen diferentes entornos de trabajo que conlleva a la contratación de productos de software básico, así como software especial para algunos departamentos, con el riesgo de abonar más de una vez el mismo producto o desaprovechar el software instalado, así mismo puede existir software desarrollado por personal de sistemas de la misma empresa que hagan mal uso y que no se aprovechen todos los recursos de este, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los centros de proceso de datos si no existen productos comunes y compatibles.

Los controles técnicos específicos, menos evidentes, son también necesarios para lograr la operatividad de los sistemas. Es decir por más pequeña que sea la aplicación que se deba ejecutar, esta debe funcionar al máximo, evitando así la inoperatividad, bien sea en hardware como en software.

Una vez conseguida la operatividad de los sistemas, el segundo objetivo de la auditoría es la verificación de la observación de las normas teóricamente existentes en el departamento de informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

a) Las normas generales de la instalación informática. Se realiza una revisión inicial sencilla, verificando la aplicación de las normas pero también registrando las áreas que no cumplan o que no las apliquen, sin olvidar que esta normativa no está en contradicción con alguna norma no informática de la empresa.

b) Los procedimientos generales informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por la persona responsable de este cargo. Tampoco el alta de una nueva aplicación podría producirse si no existieran los Procedimientos de Backup y recuperación correspondientes.

c) Los procedimientos específicos informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, explotación no debería explotar una aplicación sin haber exigido a desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los procedimientos específicos no se opongan a los procedimientos generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la normativa y los procedimientos generales de la propia empresa, a los que la informática debe estar sometida.

1.3.2 Características de la auditoría informática:[12]

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la auditoría de Inversión informática.

Del mismo modo, los sistemas informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la auditoría de seguridad informática en general, o a la auditoría de seguridad de alguna de sus áreas, como pudieran ser desarrollo o técnica de sistemas.

Cuando se producen cambios estructurales en la informática, se reorganiza de alguna forma su función: se está en el campo de la auditoría de organización informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de desarrollo de proyectos de la informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

Teniendo en cuenta lo anterior y partiendo de las diferentes actividades de sistemas que cada empresa tiene dentro de su organización dentro de las áreas generales, se establecen las siguientes divisiones de auditoría informática[13]: de Explotación, de sistemas, de comunicaciones y de desarrollo de proyectos. Estas son las áreas específicas de la auditoría informática más importantes. Cada área específica puede ser auditada desde los siguientes criterios generales, que pueden modificarse según sea el tipo de empresa a auditar:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la informática en general o la rama auditada.

1.3.3. Clasificación de la auditoría informática

Auditoría informática de explotación

Explotación informática se encarga de obtener resultados informáticos, como son: listados impresos, ficheros soportados magnéticamente, órdenes automatizadas para lanzar o modificar procesos industriales, entre otras. Los datos es la materia prima que hay que transformar por medio del proceso informático (gobernado por programas), bajo

[12] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml
[13] http://www.monografias.com/trabajos5/audi/audi.shtml

el criterio de integridad y control de calidad y así lleguen finalmente al usuario. Para auditar explotación hay que auditar las sesiones que la componen y sus interrelaciones.

Auditoría informática de sistemas: encargada de analizar todo lo concerniente a técnica de sistemas en todas sus facetas, teniendo como resultado en la actualidad que todo lo que forme el entorno general de sistemas, como son las comunicaciones, líneas y redes de la instalaciones informáticas, se auditen por separado. Dentro de la auditoria informática de sistemas se evalúa lo siguiente:

- *Sistemas operativos*: debe verificarse en primer lugar que los sistemas estén actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los sistemas operativos permite descubrir las posibles incompatibilidades entre otros productos de software básico adquiridos por la instalación y determinadas versiones de aquellas.

- *Software básico:* es fundamental para el auditor conocer los productos de software básico que han sido adquiridos aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

- *Tunning:* es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de técnica de sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados.

- *Optimización de los sistemas y subsistemas*: la técnica de sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings pre-programados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la operatividad de los sistemas ni el plan crítico de producción diaria de explotación.

- *Administración de base de datos:* el diseño de las bases de datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de técnica de sistemas, y de acuerdo con las áreas de desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. El auditor de base de datos analizará los sistemas de salvaguarda existentes, revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

- *Investigación y desarrollo*: como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las compañías del mismo

campo. La auditoría informática deberá cuidar de que la actividad de Investigación y desarrollo no interfiera ni dificulte las tareas fundamentales internas. La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los sistemas

Auditoría informática de comunicaciones y redes[14]: para el informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc. no son sino el soporte físico-lógico del tiempo real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios).

El auditor de comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (Pantallas, Servidores de redes locales, computadoras con tarjetas de comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

Auditoría informática de desarrollo de proyectos o aplicaciones: el Desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones, que a su vez, engloba muchas áreas que tiene la empresa. Una aplicación recorre las siguientes fases:

- Pre-requisitos del usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (pre-programación y programación)
- Pruebas
- Entrega a explotación y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

[14] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

***Auditoría de la seguridad informática*:** la computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes, virus, etc, que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarse en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

1.3.4 Metodología de auditoría informática. Como auditor se debe recolectar toda la información general, que permita así mismo definir un juicio global objetivo siempre amparadas en pruebas o hechos demostrables. Dar como resultado un informe claro, conciso y a la vez preciso depende del análisis y experiencia del auditor, frente a diferentes entornos a evaluar, dependiendo de las debilidades y fortalezas encontradas en dicha empresa auditada. La recolección de información, el análisis, la aplicación de diferentes normas de acuerdo al tipo de auditoría, los hallazgos encontrados y pruebas que avalen estos resultados son indispensables en la realización de una auditoria. Para llegar al resultado hay que seguir una serie de pasos que permiten tener claridad y orden de la auditoria aplicar.

El método de trabajo del auditor pasa por las siguientes etapas[15]:

1. Alcance y objetivos de la auditoría informática.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Elaboración del plan y de los programas de trabajo.
5. Actividades propiamente dichas de la auditoría.
6. Confección y redacción del informe final.
7. Redacción de la carta de introducción o carta de presentación del informe final.

Alcance y objetivos de la auditoría informática.

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del informe final.

[15] http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm#p2-1-1

Estudio inicial del entorno auditable.

Esta etapa es una de las más importantes en el desarrollo de la auditoria, ya que el auditor debe conocer todos los procesos desarrollados, relacionado con el área tomada como caso de estudio. Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

Organización: para el auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto el auditor deberá fijarse en:

Organigrama: el organigrama expresa la estructura oficial de la organización a auditar. Permite identificar las jerarquías, dependencias y direcciones entre las áreas existentes.

- ✓ Departamentos: se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.
- ✓ Relaciones Jerárquicas y funcionales entre órganos de la Organización: el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.
- ✓ Flujos de Información: además de las corrientes verticales intra -departamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra-departamentales.
- ✓ Número de puestos de trabajo: el equipo auditor comprobará que los nombres de los Puestos de trabajo de la organización corresponden a las funciones reales distintas.
- ✓ Número de personas por puesto de trabajo: es un parámetro que los auditores informáticos deben tener en cuenta ya que la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno operacional: el auditor informático debe tener una referencia del entorno en el que va a desenvolverse y se obtiene determinando lo siguiente:

- ✓ Situación geográfica de los sistemas: se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa, continuando con la verificación de la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

- ✓ Arquitectura y configuración de hardware y software: cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, para esto es importante que los auditores, en su estudio inicial, tengan en su poder la distribución e interconexión de los equipos.

- ✓ Inventario de hardware y software: el auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware

figurarán las CPU'S, unidades de control local y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

- ✓ Comunicación y redes de comunicación: al realizar el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, igualmente, poseerán información de las redes locales de la Empresa y todo lo que tenga que ver con la red de comunicaciones.

Determinación de los recursos necesarios para realizar la auditoría: mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos humanos: la cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es igualmente señalable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Recursos materiales: los recursos materiales del auditor son de dos tipos:

- ✓ Recursos software como son, cantidad y complejidad de bases de datos y ficheros, que son programas propios de la auditoria, son muy potentes y flexibles.
- ✓ Recursos materiales hardware: Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Por lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, scanner, etc.

Elaboración del plan y de los programas de trabajo: una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo y así, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

- ✓ Si la revisión debe realizarse por áreas generales o áreas específicas.
- ✓ Si la auditoría es global, de toda la informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.
- ✓ En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- ✓ En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- ✓ En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- ✓ El Plan establece disponibilidad futura de los recursos durante la revisión.
- ✓ El Plan estructura las tareas a realizar por cada integrante del grupo.
- ✓ En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el plan, se procede a la programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

Actividades propiamente dichas de la auditoría informática: la auditoría informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad. Existen técnicas que hacen que el auditor las aplique de acuerdo a su juicio y al tipo de auditoría a ejecutar y son:

Técnicas de Trabajo:

- ✓ Análisis de la información obtenida del auditado
- ✓ Análisis de la información propia
- ✓ Cruzamiento de las informaciones anteriores
- ✓ Entrevistas
- ✓ Simulación
- ✓ Muestreos
- ✓ Inspección
- ✓ Confirmación
- ✓ Investigación
- ✓ Certificación
- ✓ Observación

Herramientas:

- ✓ Cuestionario general inicial
- ✓ Cuestionario Checklist
- ✓ Estándares
- ✓ Monitores
- ✓ Simuladores (Generadores de datos)
- ✓ Paquetes de auditoría (Generadores de Programas)
- ✓ Matrices de riesgo

Confección y redacción del informe final: la función de la auditoría se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Redacción de la carta de introducción o carta de presentación del informe final: la carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrato la auditoría.

Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no hará copias de la citada carta de introducción. La carta de introducción poseerá los siguientes atributos:

- ✓ Tendrá como máximo 4 folios
- ✓ Incluirá fecha, naturaleza, objetivos y alcance
- ✓ Cuantificará la importancia de las áreas analizadas.
- ✓ Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- ✓ Presentará las debilidades en orden de importancia y gravedad.

En la carta de introducción no se escribirán nunca recomendaciones.

*Estructura del informe final: e*l informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Siguiendo los siguientes pasos:

- ✓ Definición de objetivos y alcance de la auditoría
- ✓ Enumeración de temas considerados
- ✓ Cuerpo expositivo

Para cada tema, se seguirá el siguiente orden a saber:

a) Situación actual*.* Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
b) Tendencias*.* Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c) Puntos débiles y amenazas.
d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
e) Redacción posterior de la carta de introducción o presentación.

Modelo conceptual de la exposición del informe final:

- ✓ El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- ✓ El Informe debe consolidar los hechos que se describen en el mismo.
- ✓ El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

a) El hecho debe poder ser sometido a cambios.
b) Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
c) No deben existir alternativas viables que superen al cambio propuesto.
d) La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

Hecho encontrado.

- ✓ A de ser relevante para el auditor y pera el cliente
- ✓ A de ser exacto, y además convincente.
- ✓ No deben existir hechos repetidos.

Consecuencias del hecho: las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

*Repercusión del hecho: s*e redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho: no deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

Recomendación del auditor informático

- ✓ Deberá entenderse por sí sola, por simple lectura.
- ✓ Deberá estar suficientemente soportada en el propio texto.
- ✓ Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- ✓ La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.4. HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA[16]

1.4.1 Cuestionarios. Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser habitual comenzar solicitando la cumplimentación de cuestionarios pre-impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

[16] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre-impresos hubiesen proporcionado.

1.4.2 Entrevistas. El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

1.4.3 Checklist. El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus cuestionarios, de sus checklists.

Hay opiniones que descalifican el uso de las checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de checklist. Salvo excepciones, las checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de auditoría informática guardan sus checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y concisamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango: contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo: Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

    1: Muy deficiente.
    2: Deficiente.
    3: Mejorable.
    4: Aceptable.
    5: Correcto.

    Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación de la checklist no debe realizarse en presencia del auditado. Ejm:

- ¿Existe personal específico de vigilancia externa al edificio?
  Rta/ No, solamente un guarda por la noche que atiende además otra instalación adyacente.

  <Puntuación: 1>
- Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del centro de cálculo?
  Rta/ Si, pero sube a las otras 4 plantas cuando se le necesita.

  <Puntuación: 2>
- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
  Rta/ Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.

  <Puntuación: 3>
- El personal de comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?
  Rta/ No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al jefe de explotación.

  <Puntuación: 4>

  El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. Checklist binaria: es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente. Ejemplo: Se supone que se está realizando una revisión de los métodos de pruebas de programas en el ámbito de desarrollo de proyectos.

   - ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?
     <Puntuación: 1>
   - ¿Conoce el personal de desarrollo la existencia de la anterior normativa?
     <Puntuación: 1>
   - ¿Se aplica dicha norma en todos los casos?
     <Puntuación: 0>
   - ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de bases de datos reales?
     <Puntuación: 0>

   Obsérvese como en este caso están contestadas las siguientes preguntas:

   - ¿Se conoce la norma anterior?
     <Puntuación: 0>
   - ¿Se aplica en todos los casos?
     <Puntuación: 0>

Las checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la

evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las checklists binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo.

No existen checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

1.4.4 Trazas y/o huellas. Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

1.4.5 Observación. La observación es una de las técnicas más utilizadas en la recolección de información para aplicación de una auditoria, ya que a través de diferentes técnicas y métodos de observación permite recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas. Existen diferentes tipos de observación, entre las cuales están:

- Observación directa
- Observación indirecta
- Observación oculta
- Observación participativa
- Observación no participativa
- Introspección
- Estrospección
- Observación histórica
- Observación controlada

- Observación natural

1.4.6 Inventarios. Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas.

Los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales, son:

- Inventario de software
- Inventario de hardware
- Inventario de documentos
  - Inventario de documentos administrativos
    - Manuales de la organización
    - Manuales de procedimientos administrativos
    - Manuales de perfil de puestos
    - Otros manuales administrativos
  - Inventario de documentos técnicos para el sistema
    - Manuales e instructivos técnico del hardware, periféricos y componentes del sistema.
    - Manuales e instructivos de mantenimiento físico del sistema (hardware), entre otros.

1.5. ESTANDARES DE AUDITORIA

Para la realización y ejecución de una auditoria se hace necesario aplicar normas o estándares bajo los cuales las empresas deben regirse, de allí la importancia identificar los estándares internacionales que en este caso, son:[17]

Directrices gerenciales de COBIT, desarrollado por la Information Systems Audit and Control Association (ISACA) Asociación de auditoría y control de los sistemas de información: las directrices gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y administre los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados. Uno de los objetivos de ISACA es promover estándares aplicables internacionalmente para cumplir con su visión. La estructura para los estándares de auditoría de SI brinda múltiples niveles de asesoría, como:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el código de ética Profesional de ISACA.

[17] www.adacsi.org.ar/files/es/content/146/Standards.doc

- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.

- Los poseedores de la designación de auditor certificado de sistemas de información (Certified Information Systems Auditor, CISA) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la junta de directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias, así:

1. The Management of the Control of data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA): Este modelo está basado en el concepto de roles y establece responsabilidades relacionadas con seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y responsabilidad respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

2. Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez, desarrollado por la oficina de contabilidad general de los Estados Unidos (GAO): Este modelo identifica los procesos críticos, asegurando el éxito de las inversiones en tecnología de información y comunicación electrónicas. Además los organiza en cinco niveles de madurez, similar al modelo CMM.

3. Estándares de administración de calidad y aseguramiento de calidad ISO 9000, desarrollados por la Organización Internacional de Estándares (ISO): La colección ISO 9000 es un conjunto de estándares y directrices que apoyan a las organizaciones a implementar sistemas de calidad efectivos, para el tipo de trabajo que ellos realizan.

4. SysTrust – Principios y criterios de confiabilidad de sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA: Este servicio pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

5. Modelo de evolución de capacidades de software (CMM), desarrollado por el Instituto de Ingeniería de software (SEI): Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización, con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM

es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

6. Administración de sistemas de información: una herramienta de evaluación práctica, desarrollado por la directiva de recursos de tecnología de información (ITRB): Este es una herramienta de evaluación que permite a entidades gubernamentales, comprender la implementación estratégica de tecnología de información y comunicación electrónica que puede apoyar su misión e incrementar sus productos y servicios.

7. Guía para el cuerpo de conocimientos de administración de proyectos, desarrollado por el comité de estándares del instituto de administración de proyectos: esta guía está enfocada en las mejores prácticas sobre administración de proyectos. Se refiere a aspectos sobre los diferentes elementos necesarios para una administración exitosa de proyectos de cualquier naturaleza. En forma precisa, este documento identifica y describe las prácticas generalmente aceptadas de administración de proyectos que pueden ser implementadas en las organizaciones.

8. Ingeniería de seguridad de sistemas – Modelo de madurez de capacidades (SSE – CMM), desarrollado por la agencia de seguridad nacional (NSA) con el apoyo de la Universidad de Carnegie Mellon: Este modelo describe las características esenciales de una arquitectura de seguridad organizacional para tecnología de información y comunicación electrónica, de acuerdo con las prácticas generalmente aceptadas observadas en las organizaciones.

9. Administración de seguridad de información: aprendiendo de organizaciones líderes, desarrollado por la oficina de contabilidad general de los Estados Unidos (GAO): este modelo considera ocho organizaciones privadas reconocidas como líderes respecto a seguridad en cómputo. Este trabajo hace posible la identificación de 16 prácticas necesarias para asegurar una adecuada administración de la seguridad de cómputo, las cuáles deben ser suficientes para incrementar significativamente el nivel de administración de seguridad en tecnología de información y comunicación electrónica.

1.5.1 El Modelo COBIT para auditoría y control de sistemas de información[18]

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información (Control Objectives for Information Systems and related Technology). El modelo es el resultado de

[18] http://www.channelplanet.com/index.php?idcategoria=13932

una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

"La adecuada implementación de COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado. Cualquier tipo de empresa puede adoptar una metodología COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos IT y consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos", señaló un informe de ETEK.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

1.5.2. Criterios de información de COBIT. Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

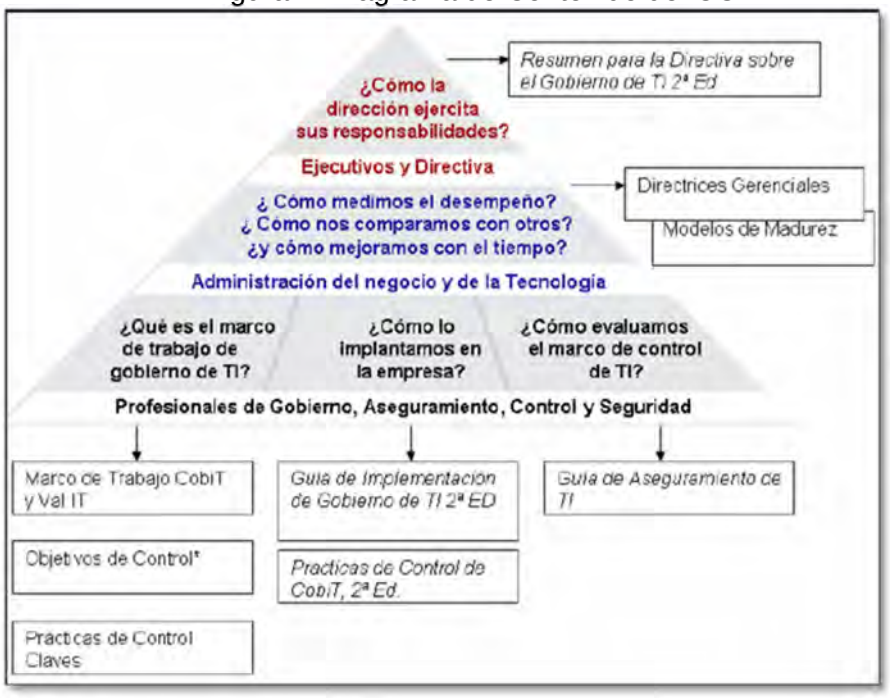
- ✓ **La efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- ✓ **La eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- ✓ **La confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.
- ✓ **La integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- ✓ **La disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

- ✓ **El cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- ✓ **La confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Los productos COBIT se han organizado en tres niveles (Figura 1), diseñados para dar soporte a lo siguiente:

• Administración y consejos ejecutivos
• Administración del negocio y de TI
• Profesionales en Gobierno, aseguramiento, control y seguridad.

Figura 1: Diagrama de Contenido del COBIT



El diagrama de contenido de COBIT mostrado en la anterior figura presenta las audiencias principales, sus preguntas sobre gobierno TI y los productos que generalmente les aplican para proporcionar las respuestas. También hay productos derivados para propósitos específicos, para dominios tales como seguridad o empresas especificas.

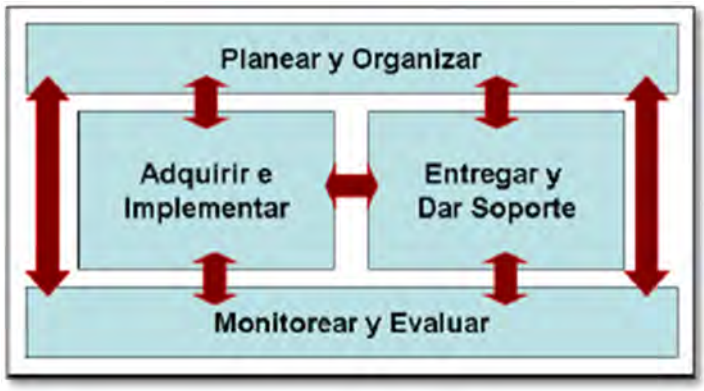
Brevemente, los productos COBIT incluyen:

- ✓ El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición: diseñado para ayudar a los ejecutivos a entender porqué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.
- ✓ Directrices gerenciales / Modelos de madurez: Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad.

- ✓ Marco de Referencia: explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.
- ✓ Objetivos de control: brindan objetivos a la dirección basados en las mejores prácticas genéricas para todas los procesos de TI
- ✓ Guía de implementación de gobierno de TI: usando COBIT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI.
- ✓ Prácticas de Control de COBIT: guía para conseguir los objetivos de control para el éxito del gobierno de TI 2ª Edición: Proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos.
- ✓ Guía de aseguramiento de TI: usando COBIT: proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia (Figura 2), que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

Figura 2: Cuadro de los dominios interrelacionados de COBIT



- ✓ *Planear y organizar (PO):* Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- ✓ *Adquirir e implementar (AI):* Proporciona las soluciones y las pasa para convertirlas en servicios.
- ✓ *Entregar y dar soporte (DS):* Recibe las soluciones y las hace utilizables por los usuarios finales.
- ✓ *Monitorear y evaluar (ME):* Monitorear todos los procesos para asegurar que se sigue la dirección provista.

- **Planificación y organización**

PO1 Definir un plan estratégico de TI
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica
PO4 Definir los procesos, organización y relaciones de TI

PO5 Administrar la inversión en TI
PO6 Comunicar las aspiraciones y la dirección de la gerencia
PO7 Administrar recursos humanos de TI
PO8 Administrar la calidad
PO9 Evaluar y administrar los riesgos de TI
PO10 Administrar proyectos

- **Adquisición e implantación**
  AI1 Identificar soluciones automatizadas
  AI2 Adquirir y mantener software aplicativo
  AI3 Adquirir y mantener infraestructura tecnológica
  AI4 Facilitar la operación y el uso
  AI5 Adquirir recursos de TI
  AI6 Administrar cambios
  AI7 Instalar y acreditar soluciones y cambios

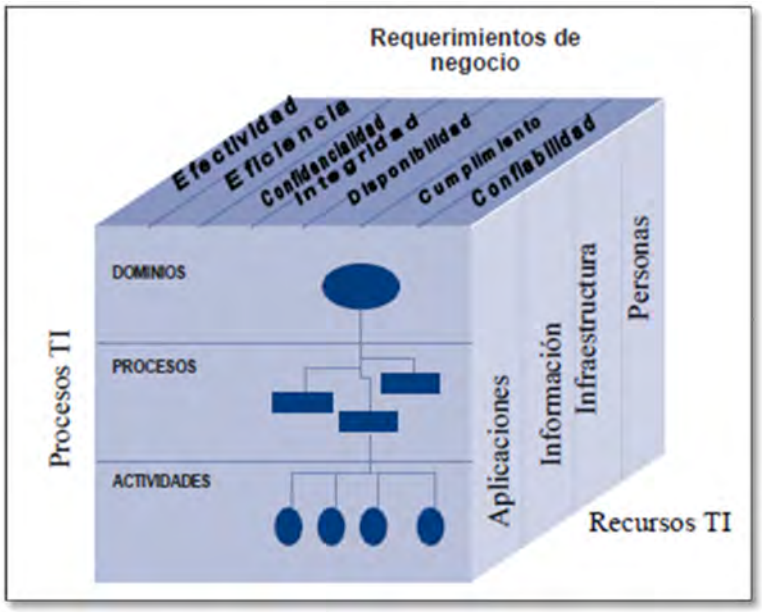
- **Soporte y Servicios**
  DS1 Definir y administrar los niveles de servicio
  DS2 Administrar los servicios de terceros
  DS3 Administrar el desempeño y la capacidad
  DS4 Garantizar la continuidad del servicio
  DS5 Garantizar la seguridad de los sistemas
  DS6 Identificar y asignar costos
  DS7 Educar y entrenar a los usuarios
  DS8 Administrar la mesa de servicio y los incidentes
  DS9 Administrar la configuración
  DS10 Administrar los problemas
  DS11 Administrar los datos
  DS12 Administrar el ambiente físico
  DS13 Administrar las operaciones

- **Monitoreo y evaluación**

  ME1 Monitorear y evaluar el desempeño de TI
  ME2 Monitorear y evaluar el control interno
  ME3 Garantizar el cumplimiento regulatorio
  ME4 Proporcionar gobierno de TI

Estos dominios agrupan objetivos de control de alto nivel (Figura 3), que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Figura 3: El cubo de COBIT



Asimismo, se debe tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

1.5.3 Dominios De COBIT. Entendiéndose como dominio, la agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional, los procesos a su vez son conjuntos o series de actividades unidas con delimitación o cortes de control y las actividades son acciones requeridas para lograr un resultado medible.

COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa.

Dominio: Planificación y organización (PO)

Este dominio cubre la estrategia y tácticas, y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos

PO1 Definición de un plan estratégico

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través de un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- ✓ La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
- ✓ El inventario de soluciones tecnológicas e infraestructura actual, deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- ✓ Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.
- ✓ Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos.

PO2 Definición de la arquitectura de información

Objetivo: satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- ✓ La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- ✓ El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización deberá ser continuamente actualizado.
- ✓ La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

PO3 Determinación de la dirección tecnológica

Objetivo: aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- ✓ La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y

debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

- ✓ El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- ✓ Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- ✓ Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI

Objetivo: prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- ✓ El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- ✓ Propiedad, custodia, la gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- ✓ Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.
- ✓ Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- ✓ Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.
- ✓ La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- ✓ Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.
- ✓ El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5 Manejo de la inversión

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través de presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- ✓ Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

- ✓ El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
- ✓ La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6 Comunicación de la dirección y aspiraciones de la gerencia

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- ✓ Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido y promovido por la Alta Gerencia.
- ✓ Las directrices tecnológicas.
- ✓ El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- ✓ El compromiso con la calidad, la gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
- ✓ Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

PO7 Administración de recursos humanos

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- ✓ El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- ✓ Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.
- ✓ La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- ✓ La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

PO8 Asegurar el cumplimiento con los requerimientos externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales.
Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- ✓ Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
- ✓ Leyes, regulaciones y contratos.
- ✓ Revisiones regulares en cuanto a cambios.
- ✓ Búsqueda de asistencia legal y modificaciones.
- ✓ Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- ✓ Privacidad
- ✓ Propiedad intelectual
- ✓ Flujo de datos externos y criptografía

PO9 Evaluación de riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI.

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- ✓ Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
- ✓ Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
- ✓ Actualización de evaluación de riesgos.
- ✓ Metodología de evaluación de riesgos.
- ✓ Medición de riesgos cualitativos y/o cuantitativos.
- ✓ Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
- ✓ Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10 Administración de proyectos

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar

y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- ✓ Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
- ✓ El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- ✓ Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- ✓ Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- ✓ Presupuestos de costos y horas hombre.
- ✓ Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- ✓ Plan de administración de riesgos para eliminar o minimizar los riesgos.
- ✓ Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad

Objetivo: satisfacer los requerimientos del cliente.
Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- ✓ Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
- ✓ Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
- ✓ Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- ✓ Documentación de pruebas de sistemas y programas.
- ✓ Revisiones y reportes de aseguramiento de calidad.

Dominio: Adquisición e implementación (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos

AI1 Identificación de soluciones automatizadas

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- ✓ Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- ✓ Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
- ✓ Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- ✓ Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
- ✓ Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso).
- ✓ Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- ✓ Aceptación de instalaciones y tecnología a través del contrato con el proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

AI2 Adquisición y mantenimiento del software aplicativo

Objetivo: Proporcionar funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- ✓ Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- ✓ Requerimientos de archivo, entrada, proceso y salida.
- ✓ Interface usuario-máquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- ✓ Personalización de paquetes.
- ✓ Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- ✓ Controles de aplicación y requerimientos funcionales
- ✓ Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizará una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- ✓ Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
- ✓ Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- ✓ Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4 Desarrollo y mantenimiento de procedimientos

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- ✓ Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- ✓ Manuales de operaciones y controles, de manera que estén en permanente actualización.
- ✓ Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 Instalación y aceptación de los sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado.

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- ✓ Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- ✓ Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- ✓ Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- ✓ Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

- ✓ Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera más económica.

AI6 Administración de los cambios

Objetivo: minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- ✓ Identificación de cambios tanto internos como por parte de proveedores
- ✓ Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- ✓ Evaluación del impacto que provocaran los cambios.
- ✓ Autorización de cambios
- ✓ Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
- ✓ Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

Dominio: Entregar y dar soporte (DS)

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos

DS1 Definición de niveles de servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido.
Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- ✓ Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
- ✓ Definición de las responsabilidades de los usuarios y de la función de servicios de información.

- ✓ Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
- ✓ Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
- ✓ Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
- ✓ Garantías de integridad
- ✓ Convenios de confidencialidad
- ✓ Implementación de un programa de mejoramiento del servicio.

DS2 Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.
Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- ✓ Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- ✓ Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
- ✓ Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- ✓ Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

DS3 Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.
Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- ✓ Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información.
- ✓ Monitoreo y reporte de los recursos de tecnología de información.
- ✓ Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- ✓ Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista

una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.
- ✓ Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

DS4 Asegurar el servicio continuo

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.
Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- ✓ Planificación de severidad
- ✓ Plan documentado
- ✓ Procedimientos alternativos
- ✓ Respaldo y recuperación
- ✓ Pruebas y entrenamiento sistemático y singulares

DS5 Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- ✓ Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.
- ✓ Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.
- ✓ Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- ✓ Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- ✓ Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- ✓ Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización.

DS6 Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.
Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- ✓ Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- ✓ Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.
- ✓ Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

DS7 Identificación y asignación de costos

Objetivo: asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI.

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- ✓ Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.
- ✓ Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades.
- ✓ Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía.

DS8 Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.

Para ello se realiza un buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- ✓ Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda.
- ✓ Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas.
- ✓ Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

DS9 Administración de la configuración

Objetivo: dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- ✓ Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
- ✓ Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración.
- ✓ Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización.
- ✓ Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

DS10 Administración de problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

DS11 Administración de datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CD y cintas magnéticas) de todas las

transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

DS12 Administración de las instalaciones

Objetivo: proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administración de la operación

Objetivo: asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

Dominio: monitoreo y evaluación (ME)

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos

M1 Monitoreo del proceso

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2 Monitorear y evaluar el control interno

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3 Garantizar el cumplimiento con requerimientos

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4 Proporcionar gobierno de TI

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.

Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoria, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

Un control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán".

Un objetivo de control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

-Los recursos de las TI.
-Los criterios empresariales que deben satisfacer la información.
-Los procesos de TI.

Para cada uno de estos 34 procesos, tiene un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades clave y entregables principales, y quién es el responsable de ellas.

1.6 MATRIZ DE PROBABILIDAD DE IMPACTO

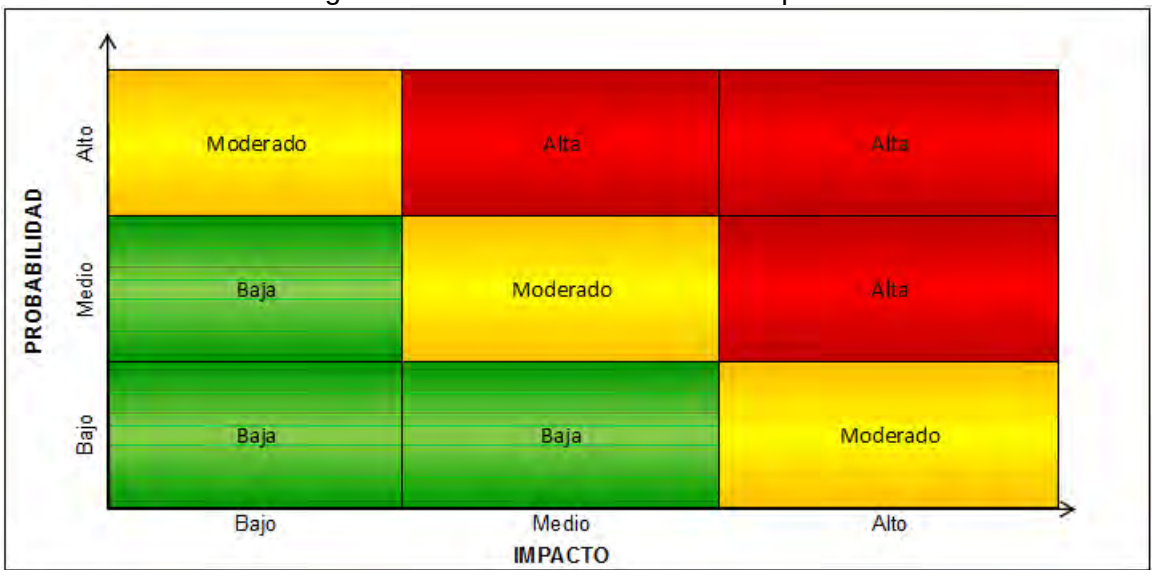
Es una forma usual de establecer o clasificar si un riesgo es bajo, medio o alto, a través de la combinación de dos dimensiones de un riesgo: su probabilidad de que suceda y el impacto que esta genere en los objetivos de la empresa si este llegara a ocurrir. La matriz de probabilidad e impacto (Figura 4), es el punto clave en clasificar los riesgos, obteniendo así:

Eje X: el impacto que el riesgo genera en los objetivos del proyecto, puede ser de impacto bajo, medio o alto.

Eje Y: la probabilidad de ocurrencia del riesgo puede ser probabilidad de ocurrencia baja, media y alta de que suceda.

El siguiente grafico representa la matriz de probabilidad e Impacto (Figura 4).

Figura 4: Matriz de Probabilidad e Impacto



Donde:

Riesgos bajos, que quizá necesitan monitorización, planes de actuación detectivos.

Riesgos Moderados, riesgos que necesitan investigación, planes de actuación preventivos.

Riesgos altos, que necesitan mitigación, planes de actuación correctivos.

1.7 DIAGRAMA DE PROCESOS

El diagrama de procesos también conocido comúnmente como diagramas de flujo de datos (DFD) es importante porque facilita la representación grafica del flujo de datos y la secuencia de un proceso, luego de un minucioso y cuidadoso análisis para el diseño de estos, lo que permite de manera audaz el rápido reconocimiento de los diferentes procesos que se desarrollan dentro de un área o sistema de una empresa.

Diagrama de flujo[19]

Es la representación gráfica del algoritmo o proceso. Se utiliza en disciplinas como la programación, la economía, los procesos industriales y la psicología cognitiva. Estos diagramas utilizan símbolos con significados bien definidos que representan los pasos del algoritmo, y representan el flujo de ejecución mediante flechas que conectan los puntos de inicio y de fin de proceso.

[19] http://es.wikipedia.org/wiki/Diagrama_de_flujo

Características:

Un diagrama de flujo siempre tiene un único punto de inicio y un único punto de término. Las siguientes son acciones previas a la realización del diagrama de flujo:

- Identificar las ideas principales a ser incluidas en el diagrama de flujo. Deben estar presentes el dueño o responsable del proceso, los dueños o responsables del proceso anterior y posterior y de otros procesos interrelacionados, otras partes interesadas.
- Definir qué se espera obtener del diagrama de flujo.
- Identificar quién lo empleará y cómo.
- Establecer el nivel de detalle requerido.
- Determinar los límites del proceso a describir.

Los pasos a seguir para construir el diagrama de flujo son:

- Establecer el alcance del proceso a describir. De esta manera quedará fijado el comienzo y el final del diagrama. Frecuentemente el comienzo es la salida del proceso previo y el final la entrada al proceso siguiente.
- Identificar y listar las principales actividades/subprocesos que están incluidos en el proceso a describir y su orden cronológico.
- Si el nivel de detalle definido incluye actividades menores, listarlas también.
- Identificar y listar los puntos de decisión.
- Construir el diagrama respetando la secuencia cronológica y asignando los correspondientes símbolos.
- Asignar un título al diagrama y verificar que esté completo y describa con exactitud el proceso elegido.

Ventajas de los diagramas de flujo

- Favorecen la comprensión del proceso al mostrarlo como un dibujo. El cerebro humano reconoce muy fácilmente los dibujos. Un buen diagrama de flujo reemplaza varias páginas de texto.
- Permiten identificar los problemas y las oportunidades de mejora del proceso. Se identifican los pasos, los flujos de los re-procesos, los conflictos de autoridad, las responsabilidades, los cuellos de botella, y los puntos de decisión.
- Muestran las interfaces cliente-proveedor y las transacciones que en ellas se realizan, facilitando a los empleados el análisis de las mismas.
- Son una excelente herramienta para capacitar a los nuevos empleados y también a los que desarrollan la tarea, cuando se realizan mejoras en el proceso.
- Al igual que el pseudocódigo, el diagrama de flujo con fines de análisis de algoritmos de programación puede ser ejecutado en un ordenador, con un IDE como Free DFD.

Tipos de diagramas de flujo

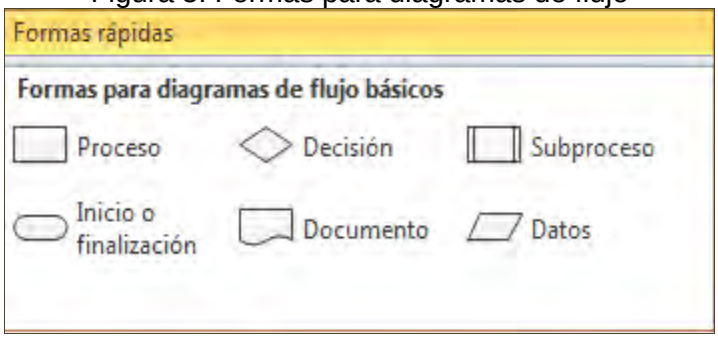
- Formato vertical: en él, el flujo o la secuencia de las operaciones, va de arriba hacia abajo. Es una lista ordenada de las operaciones de un proceso con toda la información que se considere necesaria, según su propósito.

- Formato horizontal: En él, el flujo o la secuencia de las operaciones, va de izquierda a derecha.
- Formato panorámico: el proceso entero está representado en una sola carta y puede apreciarse de una sola mirada mucho más rápido que leyendo el texto, lo que facilita su comprensión, aún para personas no familiarizadas. Registra no solo en línea vertical, sino también horizontal, distintas acciones simultáneas y la participación de más de un puesto o departamento que el formato vertical no registra.
- Formato arquitectónico: describe el itinerario de ruta de una forma o persona sobre el plano arquitectónico del área de trabajo. El primero de los flujogramas es eminentemente descriptivo, mientras que los utilizados son fundamentalmente representativos.

Simbología y significado

Se utiliza símbolos para mostrar el flujo de las diferentes acciones y decisiones involucradas en el proceso (Figura 5), así:

Figura 5: Formas para diagramas de flujo



Inicio-Finalización: es un ovalo que se utiliza para representar el Inicio o Fin de un algoritmo del proceso.

Proceso: un cuadrado o rectángulo que representa la actividad desarrollada, una instrucción o cualquier tipo de operación que origine un cambio de valor en el proceso.

Decisión: un rombo, utilizado para la toma de decisiones, a través de indicaciones de operaciones lógicas o de comparación entre datos que determina el flujo a seguir dentro del proceso.

Subproceso: rectángulo con doble línea que determina los pasos o actividades que se incluyen dentro del proceso.

Documento: figura documento que determina la cantidad de documentos y copias de los mismos que se requieren en el proceso.

Datos: figura que representa la entrada o salida de información que sea procesada o registrada.

2. DESARROLLO DE LA AUDITORIA

2. 1 METODOLOGÍA

Las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada eficaz, razón por la que la metodología utilizada para la realización de la auditoria de sistemas dentro de Emssanar E.S.S es de tipo cuantitativo/subjetivo, basados en un modelo matemático numérico, arrojando como resultado una lista de riesgos obtenidos del análisis de cada uno de los procesos a auditar teniendo en cuenta su importancia e impacto dentro del área de sistemas de ahí su calificación y recomendaciones realizadas.

La metodología aplicada en la realización de esta auditoría, se ejecuto de la siguiente manera:

Etapa1. Exploración del entorno

Este primer paso se realizó con el fin de familiarizarse con el área de sistemas de la entidad Emssanar E.S.S, se hace un estudio previo de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoria, también en esta etapa se definen que elementos se utilizaron para elaborar la auditoria.

Se realizaron varias visitas a la sede principal Emssanar E.S.S con el fin de conocer y observar los diferentes procesos, para identificarlos y auditarlos, a través de entrevistas abiertas se dio inicio a la recolección de información, dando el siguiente paso que fueron la aplicación de cuestionarios cuantificables con los funcionarios de los diferentes departamentos, como también la visita a las diferentes sedes que tiene Emssanar, así:

- Sede Principal Emssanar E.S.S
- Emssanar I.P.S
- Laboratorio Clínico Emssanar
- Fundación Emssanar
- Cresemillas (SIAU Atención al Usuario y CC Centro de Contactos)
- IPS Lorenzo.

También se visitaron la zonal que en este caso es el municipio de Ipiales y como municipal el municipio de Córdoba.

Etapa2. Planeación de las actividades de auditoria

Aquí se realizó la planificación de todo el proceso de la auditoría, con las siguientes actividades:

- Se realizó un estudio previo del área de sistemas de Emssanar ESS obteniendo información necesaria respecto al tema.
- Se identificó el alcance y los objetivos de la auditoria a realizar.

- Determinación de los recursos necesarios con los que se realizó la auditoria.
- Se elaboró el plan de trabajo.

Etapa3. Realización las actividades de la auditoria

En esta etapa se realizaron las diferentes actividades implantadas en la etapa anterior, mediante la aplicación de técnicas junto con la aplicación de diferentes herramientas que garantizo el cumplimiento de los objetivos propuestos para la ejecución de la auditoria. En esta etapa se realizaron las siguientes actividades:

- Elaboración del plan de auditoría, a través de COBIT permitiendo así la identificación de los procesos y objetivos de control evaluados.
- Se elaboran cuadros de definición de fuentes de conocimiento, que facilitan la identificación clara de la fuente de obtención de las pruebas.
- Se aplicaron entrevistas con preguntas abiertas y preguntas cerradas para la obtención de información general de la empresa, para luego elaborar diferentes cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT a auditar.
- Identificación de hallazgos.
- Mediante el formato de hallazgos, se asigna la probabilidad de ocurrencia e impacto para los riesgos encontrados.
- Elaboración de la matriz de probabilidad e impacto, que permitió identificar los riesgos altos que necesitan mitigarse de manera urgente mediante un plan correctivo.

Etapa 4. Presentación del informe final

Etapa en la cual se realizó el informe final que contiene todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa o los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo.

Este informe se presento y se entrego al personal de la jefatura del área de sistemas de la sede principal Emssanar E.S.S, para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

2.2 ARCHIVO PERMANENTE

Se incluye en este punto información permanente que sirve de consulta guía para la evaluación de políticas y procedimientos de la empresa, en este caso de Emssanar ESS.

2.2.1. Ambiente general de la empresa

Información general y ubicación

La empresa solidaria de salud EMSSANAR ESS, es una institución prestadora de servicios de salud de primer y segundo nivel de complejidad con cobertura geográfica en

Nariño, Putumayo, Cauca y Valle, siendo una empresa de carácter social del Estado. La auditoria se ejecuto en la regional Nariño, ubicada en la ciudad de Pasto. Sede principal situada en:

- Dirección: B/San Ignacio
- Teléfono: 7336030 ext. 103318
- Pagina web: www.emssanar.org.co
- e-mail: corporativa@emssanar.org.co

Emssanar siempre se ha preocupado por mantenerse en los primeros lugares, ya que tiene diferentes proyectos sociales enfocados hacia la problemática en salud. Desarrolla cinco programas entre ellos 'Vivamos sin VIH', 'Riñones sanos', 'Disminuyamos la mortalidad perinatal', 'Prevengamos el Cáncer' y 'Maternidad Segura', que se han socializado en las comunidades. En el aspecto social, trabaja con 38 organizaciones de asociados que tienen sus proyectos productivos en zonas rurales, generalmente alejadas de las cabeceras municipales. También participa en capacitación, a través de un Centro de Estudios Técnicos, que beneficia a los asociados y afiliados, en carreras tecnológicas. En cuanto a la relación con los entes territoriales, es excelente porque mantiene buena comunicación, de tal manera que las respuestas frente a la problemática que se genera dentro del aseguramiento, han sido concertadas. Y, con los hospitales, tiene una relación de confianza, a pesar de que muchas veces el flujo de recursos no es el ideal. Sin embargo, ellos permiten que las negociaciones sean las más adecuadas y que participe también en algunas de sus actividades en salud, sociales o deportivas.

Emssanar es una Empresa Promotora de Salud del Régimen Subsidiado que integra a mas de 1.200.000 mil afiliados en el sur occidente colombiano; cuenta con una red de 270 IPS en los departamentos de Nariño, Putumayo, Cauca y Valle, integradas a través de un innovador Centro de Contactos que permite mejorar la atención al usuario.

Historia de Emssanar ESS [20]

Desde una Empresa Solidaria de Salud a un Grupo Empresarial y Comunitario en el Sur Occidente Colombiano.

1990, Colombia en el Sistema Nacional de Salud, un escenario donde se encontraban criticas alusivas a: "el sistema actual convierte a los individuos y comunidades en sujetos pasivos de sus actividades y no permite que esas comunidades ejerzan el derecho a cuidar de su salud y a recibir y exigir del sistema servicios oportunos y de buena calidad".

Frente a este escenario el gobierno Nacional propuso el programa de Empresas Solidarias de Salud como respuesta a las necesidades del sector, como lo describe Iván Jaramillo "Las Empresas Solidarias de Salud se crearon antes de la ley 100 de 1993 y según el Ministro de Salud, Juan Luis Londoño, la experiencia que sirvió de base fue la de los hogares comunitarios del ICBF, los cuales con el mismo dinero lograron multiplicar mas la cobertura … según las cuales la transformación de los subsidios en demanda permite focalizar mejor los subsidios estatales, sustituir a las entidades públicas

[20] http://www.emssanar.org.co/contenidos/COOEmssanarIPS/rendicion_de_cuentas/CODIGO_DE_BUEN_GOBIERNO_Y_ETICA.pdf

“ineficientes y costosas” e incorporar al mercado a la población sin capacidad de compra…la ley 100 de 1993, dio origen al concepto de Régimen Subsidiado de Aseguramiento en Salud y los subsidios a la demanda se convirtieron en UPC-S / POS-S o pólizas de aseguramiento”.

Para ese entonces, el Ministerio de Salud definió una estrategia conocida como Familias Sanas en Ambientes Sanos y el Programa denominado Empresas Solidarias de Salud, dirigido a desarrollar la primera etapa conocida como gestión sanitaria, donde se planteó un modelo de atención en salud para recuperar la convivencia pacífica, el respeto por la diferencia, el trato personal e integral continuo de los individuos en el entorno familiar fundamentado en el auto-cuidado.
Considerando a la familia como el primer asegurador de salud y protección social que tendría la capacidad de resolver problemas de muy baja complejidad, donde la madre actuaba como promotora de salud por naturaleza.

Así EMSSANAR E.S.S, nace en la segunda fase del programa denominada Gestión Empresarial, donde se identificaron líderes que representaban a grupos familiares de base, cada uno constituido por veinte grupos en el que el representante o delegado se integraba a procesos organizativos comunitarios para conformar las Empresas solidarias de salud, en función, principalmente de los siguientes propósitos:

El adquirir servicios de salud con la financiación del subsidio directo otorgado por el Estado y la articulación con el Sistema General de Seguridad Social en Salud, que inicia la labor de administración de los recursos con enfoque de riesgo.
El proceso de fortalecimiento y participación, que como resultado quedó la organización y constitución de las Empresas Solidarias de Salud, el cuidado del medio ambiente, donde se conformaron los grupos extramurales de apoyo a las familias en su territorio y realidad; bajo esta idea se desarrollaron diferentes experiencias en Colombia, donde comunidades organizadas accedían a servicios de salud básica, mediante un paquete financiado con los aportes del Ministerio de Salud, los Departamentos, los Municipios y la población vinculada a dichos procesos.

En el país se constituyen diversas Empresas solidarias de salud en la región del sur occidente Colombiano como: Cuaspud Carlosama, Mutual de la Cruz, Asociación Mutual Nuevo Amanecer AMUNA, Emssanar, Alcatraz, Mallamás, Guaitará, Coopsosafa, Essalud, Coopsacoop, Coopesac y Coosalud para referirnos entre otras que se crearon en los departamentos de Nariño, Putumayo, Cauca, Valle y el resto del país. Se caracterizaban fundamentalmente por operar en los sitios de origen como generadoras de una dinámica socio-económica local.
Posteriormente, la Ley marco que creó el Sistema General de Seguridad Social, estipulo que los recursos del subsidio en salud pueden ser administrados por organizaciones de naturaleza, pública, privada, mixta o comunitaria; que se denominarían empresas promotoras de salud comunitarias.

En continuidad con el programa “Empresa Solidarias de Salud” les proporciono asistencia técnica, financiación y preferencias legales para la contratación por su naturaleza solidaria y comunitaria, brindando de esta forma un claro apoyo para el desarrollo empresarial de estas organizaciones. Sin embargo a nivel territorial y local existía desarticulación y

desmotivación para implementar el programa, encontrando diferentes obstáculos para su ejecución y desarrollo empresarial.
Para el año de 1995 se expide el Decreto 2357, que define unas condiciones para operar en el Régimen Subsidiado, nominando a todas las empresas operadoras en Administradoras del Régimen Subsidiado ARS; además de condicionar y limitar el número de afiliados en cinco mil al inicio de la operación de una ESS e incrementarlos a diez mil en el primer año, veinticinco mil en el segundo año y cincuenta mil al tercer año; además de mantener un patrimonio de cien s.m.l.v por cada cinco mil afiliados, contratar una póliza para enfermedades de alto costo y administrar los recursos a través de una Fiduciaria.

Ante la imposibilidad de alcanzar el número de afiliados requerido, las empresas solidarias de salud ESS, se ven obligadas a organizar convenios empresariales para cumplir las exigencias del Decreto, sin que cada una de ellas pierda su personería jurídica y la autonomía administrativa y financiera. Abonando el terreno para la unidad empresarial que sería requerida posteriormente.
Con esta normatividad las empresas solidarias de salud, salen del contexto municipal y se les obliga a expandirse con el fin de cumplir con los requerimientos antes mencionados, perdiendo especialmente la cercanía con las familias que inicialmente las conformaron.

En 1998 se expide el Decreto 1804, que exige a las organizaciones que deseen continuar en el Régimen Subsidiado, tener: mínimo doscientos mil afiliados, un patrimonio de diez mil s.m.l.v. contar con una plataforma tecnológica óptima, una estructura administrativa y financiera con un sistema de información y un sistema de garantía de la calidad que ofrezca acceso real para cumplir con el aseguramiento en salud de los afiliados al Régimen Subsidiado.

Este nuevo escenario se convierte en una amenaza que implicaba la desaparición de estas empresas comunitarias en el Sistema; decidiendo entre estas, asumir el reto de conformar una sólida Empresa Solidaria de Salud a través de la figura de la Incorporación, que operaría en los departamentos de Nariño, Valle, Cauca y Putumayo, permitiendo de esta forma el surgimiento de la organización EMSSANAR.

El proceso de desarrollo empresarial y comunitario definió en el año 2000, la plataforma estratégica, estableciendo un norte común" ser en el 2007 la organización comunitaria más exitosa y reconocida del país". Como parte del proceso de consolidación y en vista del éxito de la organización sumado con las oportunidades del mercado y buscando el beneficio de la comunidad, se da la apertura a nuevas unidades de servicio sociales:

IPS Ltda. Instituciones prestadoras de servicios de salud de menor complejidad.
SF Ltda. Servicio Farmacéutico con un depósito de medicamentos y el suministro para los afiliados a través de dispensarios.

Viendo la necesidad de articular el crecimiento empresarial con el desarrollo comunitario, la organización Emssanar crea para sus grupos de interés, en el momento priorizados: afiliados y asociados; la Fundación EMSSANAR para el fomento de procesos de desarrollo social y comunitario, buscando que responda al crecimiento sostenible de sí misma como a su misión social.

En la búsqueda de contar con un circuito económico solidario, que integre realmente a todos aquellos participantes de la organización, incluidos los trabajadores, se transforman la IPS Ltda. Y la SF Ltda. En Cooperativas donde, se da cabida a los trabajadores como asociados de la organización con el fin de adelantar acciones entorno a la Responsabilidad Social Empresarial.

De esta manera Emssanar se ha posicionado como organización comunitaria y empresa solidaria en la región, asegurando la salud de más de un millón de afiliados en ochenta y nueve municipios de los Departamentos de Valle, Cauca, Nariño y Putumayo, con redes de IPS y de farmacias que actúan en diferentes municipios de la región, contando cuatro mil quinientos asociados y setecientos trabajadores en sus empresas.

Esta es la historia de la organización comunitaria Emssanar, que ha iniciado un proceso, buscando irradiar en su área de influencia, no sólo el crecimiento empresarial, sino el desarrollo de región, apoyando el desarrollo endógeno de sus comunidades y permitiendo el mejoramiento de las condiciones y calidad de vida, tanto de sus asociados como de sus afiliados y trabajadores
Hoy pensamos en prospectiva ser "En el 2019 el Grupo Empresarial de la Economía Solidaria que genera capital social y desarrollo económico para el país".

Empresas Prestadoras De Salud E.P.S[21]

La salud es una de las cosas más importantes en la vida de las personas, pues gracias a esta es posible realizar en la vida todas aquellas actividades que hacen parte del diario vivir y las cuales permiten tener una vida plena, por lo tanto para mantener una buena salud que permita que las condiciones de vida estén en optimas condiciones, lo más adecuado es recurrir a las entidades que prestan los servicios de salud y que dan cabida a mantener un nivel adecuado de salud previniendo o tratando las diferentes enfermedades y atendiendo casos de accidentes, así las EPS son uno de los mayores sustentos que tienen a disposición la sociedad para contar con una buena salud.

Las EPS juegan un papel de vital importancia dentro de la sociedad, EPS hace referencia a las entidades prestadoras de salud, las cuales pueden ser tanto empresas como instituciones de naturaleza privada o pública, las cuales brindan una completa protección en salud, al permitir a sus usuarios el acceso a diferentes medios de atención, por medio de citas medicas de carácter preventivo, tratamientos y terapias, a partir de lo cual se dictan recetas medicas y se brindan medicamentos, también se atienden casos de urgencias, citas odontológicas y muchos otros medios de prestación de servicios de salud, de tal forma son muchas las maneras de brindar los servicios que se derivan de la definición de EPS.

En razón a las condiciones propias que caben dentro de la definición de EPS, se puede decir que las EPS pueden contar en ciertas ocasiones con una infraestructura propia y en muchos otros casos les pertenecen a terceros, además las EPS pueden contar con una única sede, pero dentro de la definición de EPS también es posible que la entidad se encuentre distribuida en una gran red con una sede principal y diferentes puntos de

[21] http://www.articulo.org/articulo/9219/definicion_de_eps.html
http://www.articulo.org/1/admin

atención distribuidos en puntos estratégicos de una ciudad o de un territorio, lo que permite una mayor cobertura para la prestación de los servicios de salud y mejores condiciones para los diferentes usuarios, vale la pena resaltar que estas se encuentran vigiladas o sujetas a controles, para que cumplan con ciertas condiciones de calidad, así de esta función de vigilancia sobre las EPS se encuentran las superintendencias encargadas de la salud, las cuales son una manera de manifestación del gobierno.
Entre las principales ventajas que se pueden ubicar en la definición de EPS, se destacan:

• Los usuarios de las EPS, tiene a su disposición una gran alternativa de servicios y planes de atención en salud, los cuales además deben ser de la más alta calidad y competencia, lo cual en la definición de EPS favorece a la búsqueda de mejorar cada día en la prestación de servicios.
• De la definición de EPS, se desprende la idea de planes de educación en salud, buscando ante toda la prevención de las enfermedades con citas médicas, campañas de vacunación, evitando posibles complicaciones y avance de las enfermedades.
• Mayor cobertura, como atención de enfermedades preexistentes, salud mental, dental, atención en nutrición y dietética, amplia atención de casos de embarazo y periodo de lactancia, entre muchos otros medios de prestaciones en salud.

2.2.2. Misión[22]. Emssanar E.S.S es una organización empresarial de la economía solidaria, con proyección nacional e internacional, que desde el sur occidente colombiano presta servicios en las áreas de: salud, educación técnica, comercialización de alimentos, asistencia técnica socio-empresarial y micro crédito. A través de tecnologías flexibles, el eficiente manejo de los recursos y un talento humano competente y motivado, comprometido con el liderazgo, la solidaridad, la responsabilidad social y en la contribución al mejoramiento de las condiciones de vida de su comunidad para el desarrollo del país.

2.2.3 Visión[22]. Emssanar E.S.S en el 2019 será un grupo empresarial de la economía solidaria reconocido por su aporte en la generación de capital social y desarrollo sostenible del país.

2.2.4 Valores[22]. Liderazgo, solidaridad, responsabilidad social.

2.2.5 Objetivo social[22]. EMSSANAR ESS tendrá como objeto el promover el desarrollo humano integral de sus asociados y de manera especial el organizar y garantizar la prestación integral de los servicios de salud especialmente los definidos en los regímenes de salud contributivo y subsidiado del sistema general de seguridad social, cuando las condiciones legales, administrativas, técnicas y financieras lo permitan y con los criterios de calidad de acuerdo con los principios contenidos en la Constitución Nacional, La Ley 100 de 1993, La Ley 1122 de 2007, los Decretos Reglamentarios y las normas que los modifiquen, complementen o adicionen.

Igualmente, tendrá como objeto social el promover y acompañar procesos de organización y participación comunitaria con criterios de autogestión.

[22] PORTAFOLIO_ESS.pdf

El objeto social lo desarrollará con base en una eficiente administración de los recursos que el Estado en sus diferentes niveles destine para tal fin, los aportes de los asociados y otros que la asociación pueda captar.

Los alcances y límites de los servicios de salud serán los que establezcan las normas legales vigentes que regulan el Sistema General de Seguridad Social en Salud y los que se establezcan por la Asociación y sus órganos de dirección.

En el cumplimiento de su objeto social, EMSSANAR ESS respetará la cultura, los valores, derechos, usos y costumbres de todos los asociados y en especial los de las comunidades indígenas, afrocolombianas y demás minorías étnicas.

Para el cumplimiento de su objeto social, EMSSANAR ESS, podrá desarrollar las siguientes actividades:

1. Prestar los servicios de aseguramiento en salud a través de la coordinación, organización, administración de servicios en el Sistema General de Seguridad Social con enfoque de promoción de la salud y prevención de la enfermedad.

2. Promover la afiliación de la población al Sistema General de Seguridad Social en Salud, garantizando la libre elección por parte del afiliado en su ámbito geográfico y régimen de influencia.

3. Administrar el riesgo financiero, la gestión del riesgo en salud, la articulación de los servicios que garantice el acceso efectivo, el aseguramiento de la calidad en la prestación de los servicios de salud y la representación del afiliado ante los demás actores sin perjuicio de la autonomía del usuario.

4. Afiliar a la población beneficiaria de subsidios, así como la que pertenezca al Régimen Contributivo y entregar el carné correspondiente que lo acredita como afiliado, en los términos fijados por las normas vigentes.

5. Administrar recursos públicos y privados, nacionales, departamentales, municipales e internacionales y los que aporten los asociados con el fin de dar cumplimiento a su objeto social.

6. Informar al beneficiario sobre aquellos aspectos relacionados con el contenido de los Planes de beneficios en los regímenes subsidiado y contributivo del Sistema General de Seguridad Social en Salud de acuerdo con los procedimientos para la inscripción, redes de servicios con que cuenta, deberes y derechos, así como el valor de las cuotas moderadoras y copagos que debe pagar.

7. Organizar y garantizar la prestación de los servicios de salud a los beneficiarios de subsidios, previstos en los Planes Obligatorios de Salud para lo cual adelantará los procesos de afiliación, registro y carnetización, organización, contratación del aseguramiento y prestación de los servicios de los planes de beneficios en condiciones de calidad, administración del riesgo y defensa de los derechos de los usuarios.

8. Asegurar los riesgos derivados de la atención de enfermedades de alto costo, calificadas por el Consejo Nacional de Seguridad Social, de acuerdo con las condiciones señaladas en las normas vigentes.

9. Establecer el sistema y la estructura de la administración financiera de los recursos provenientes del subsidio a la demanda.

10. Formular y organizar estrategias destinadas a proteger la salud de sus beneficiarios, que incluya las acciones de Promoción de la salud y Prevención de la enfermedad.

11. Informar a los órganos de dirección, administración, inspección y vigilancia del Estado y demás autoridades correspondientes las irregularidades que se presenten en la operación del Sistema General de Seguridad Social en Salud, en especial aquellos aspectos relacionados con los procesos de identificación, focalización, afiliación y carnetización de los afiliados a los Planes de Beneficios, independientemente de las acciones internas que se adelanten para establecer las responsabilidades personales o institucionales y para la adopción de los correctivos correspondientes.

12. Buscar la financiación y apoyo para la ejecución de programas en salud, culturales, educativos, ecológicos, deportivos, recreativos, funerarios y de vivienda, así como otros encaminados al logro del desarrollo humano integral de sus asociados en el ámbito de la seguridad social y de la economía solidaria.

13. Realizar estudios, investigaciones o programas y ejecutar proyectos contratados por entidades públicas o privadas, nacionales o internacionales, relacionados con la seguridad social y de la economía solidaria.

2.2.6 Servicios que ofrece[23]. Emssanar como grupo empresarial, es una organización comunitaria que hace parte del sector de la economía solidaria, se encuentra al servicio de la comunidad y contribuye a la construcción de la región sur occidental colombiana a través del desarrollo empresarial y la redistribución social. Conformada por diferentes servicios como son:

- ✓ **Emssanar EPS-S:** Empresa Promotora de Salud del régimen subsidiado que integra más de un millón de afiliados en el sur occidente colombiano, cuenta con una red de 270 IPS en los departamentos de Nariño, Putumayo, Cauca y Valle, integradas a través de un innovador centro de contactos que permite mejorar la atención al usuario.
- ✓ **CooEmssanar IPS:** presta servicios de salud bajo el enfoque de mejoramiento continuo y con énfasis en el paciente y su familia, garantizando la calidad en la atención caracterizada por la accesibilidad, oportunidad, seguridad, pertinencia y continuidad, mediante un modelo de salud preventivo y seguro. La política de calidad y seguridad define que el paciente recibirá cuidados en salud sin ser lesionado durante el proceso de atención de las personas que prestan los servicios.
- ✓ **CooEmssanar SF:** presta servicios dedicados al suministro de medicamentos, material médico-quirúrgico, productos cosméticos y de uso personal, en el sur occidente colombiano, garantizando su calidad son responsabilidad, actitud de servicio

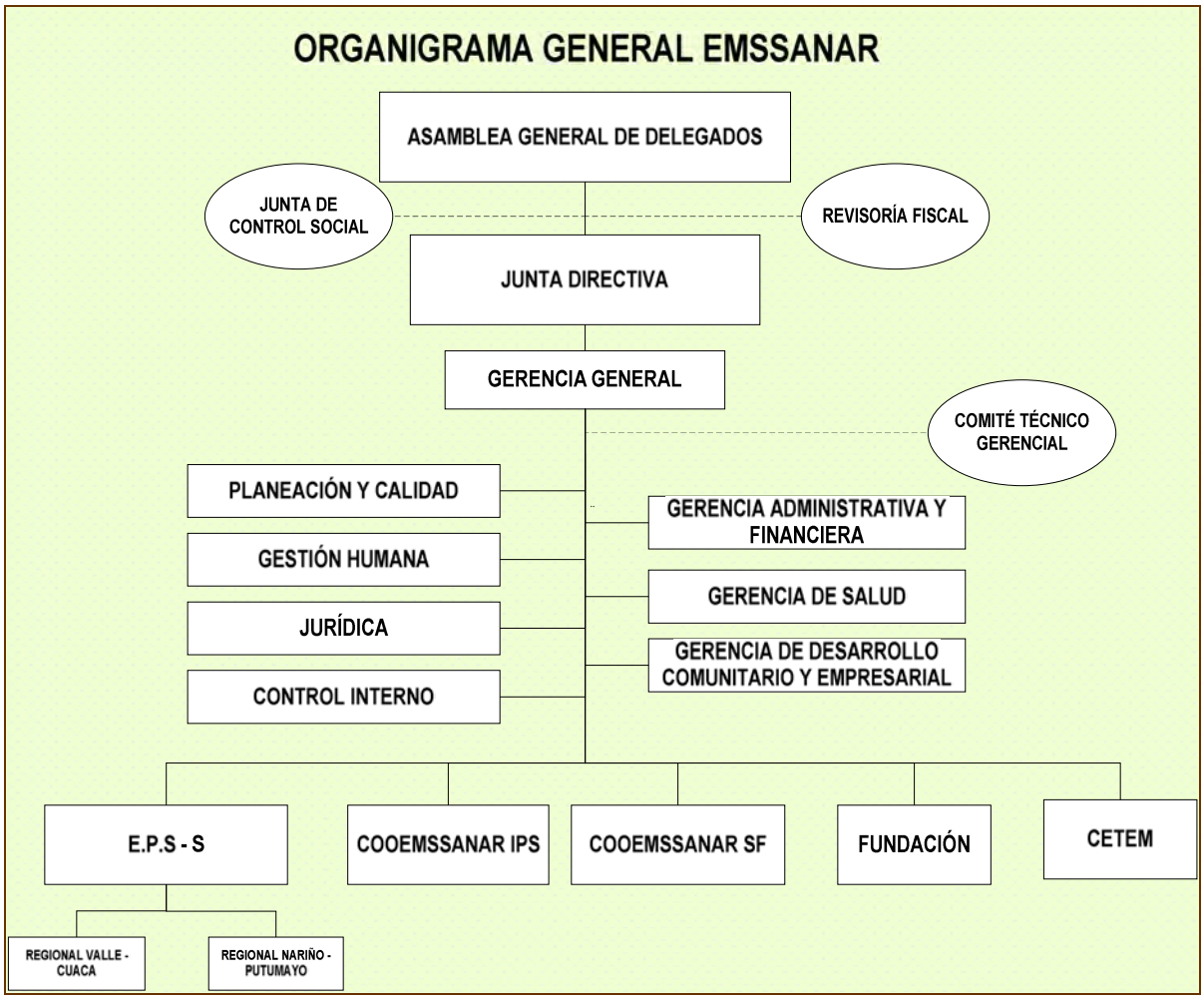
[23] PORTAFOLIO_ESS.pdf

y liderazgo, mediante un talento humano calificado y acreditado, generando confianza en nuestros clientes.

- ✓ **Fundación Emssanar:** creada como organización solidaria de desarrollo, tiene diferentes líneas de acción: acompañamiento socio empresarial, educación, investigación y comercialización social de alimentos; en cuyo marco se han ejecutado proyectos que posibilitan la proyección de la organización en la atención a población pobre y vulnerable de los departamentos de Nariño, Putumayo, Cauca y Valle.
- ✓ **Fundación de servicios educativos de Emssanar (CETEM):** entidad sin ánimo de lucro que busca contribuir al mejoramiento de las condiciones y calidad de vida de la población beneficiaria con programas, planes y proyectos de formación, capacitación y educación.

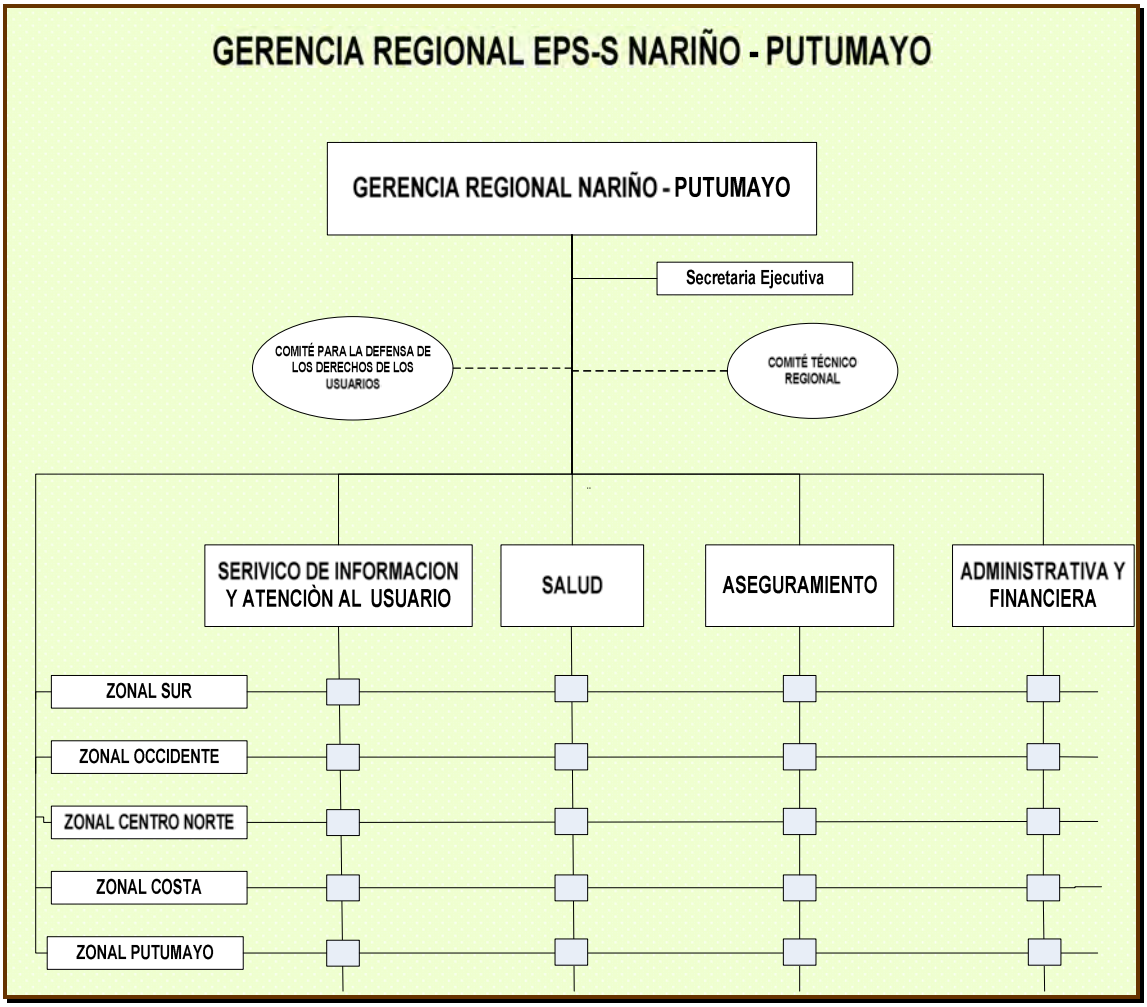
2.2.7. Organigrama general de Emssanar. Aprobación**:** según resolución de gerencia general 009 De 2.009 (Figura 6).

Figura 6: Organigrama general de Emssanar



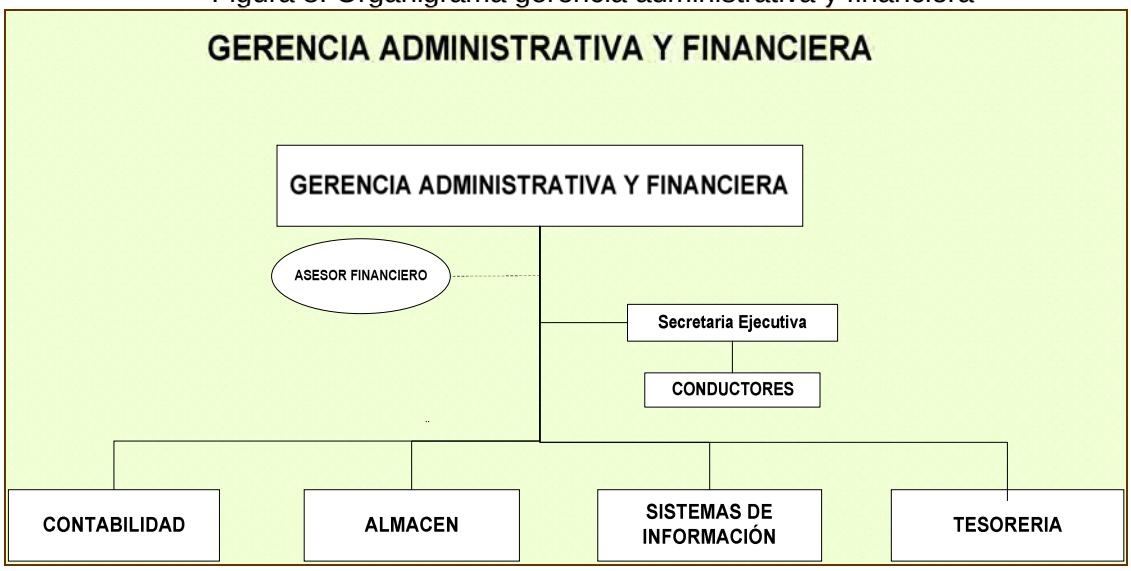
Organigrama gerencial EPS-S Nariño-Putumayo: aprobación: según resolución de gerencia general 009 De 2.009 (Figura 7).

Figura 7: Organigrama general EPS-S Nariño- Putumayo



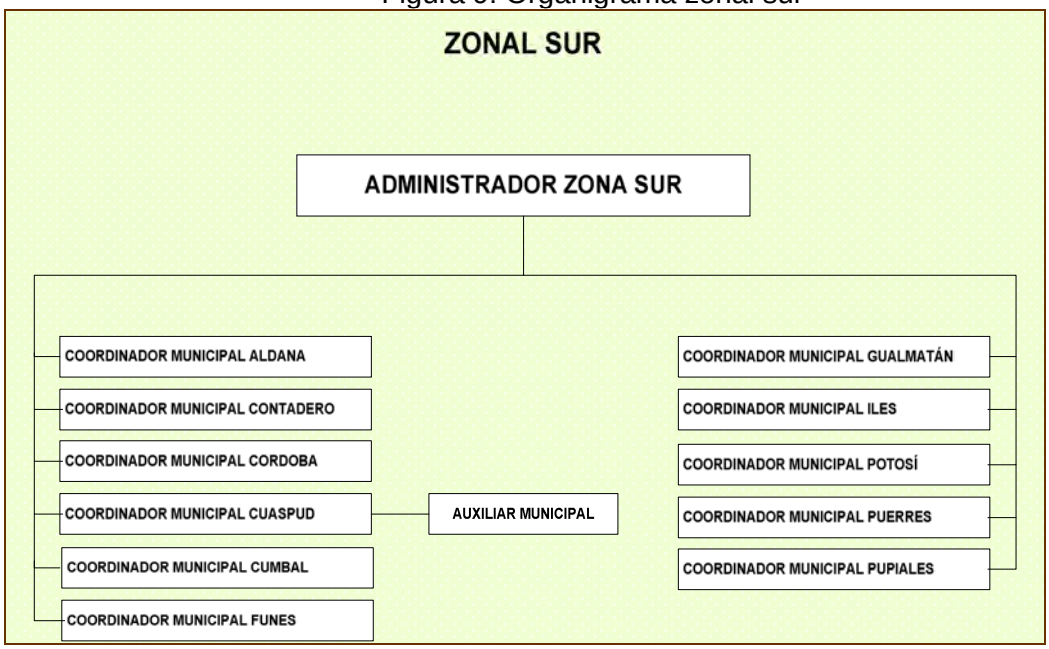
Organigrama gerencia administrativa y financiera: según resolución de gerencia general 0011 de 2.009 (Figura 8).

Figura 8: Organigrama gerencia administrativa y financiera



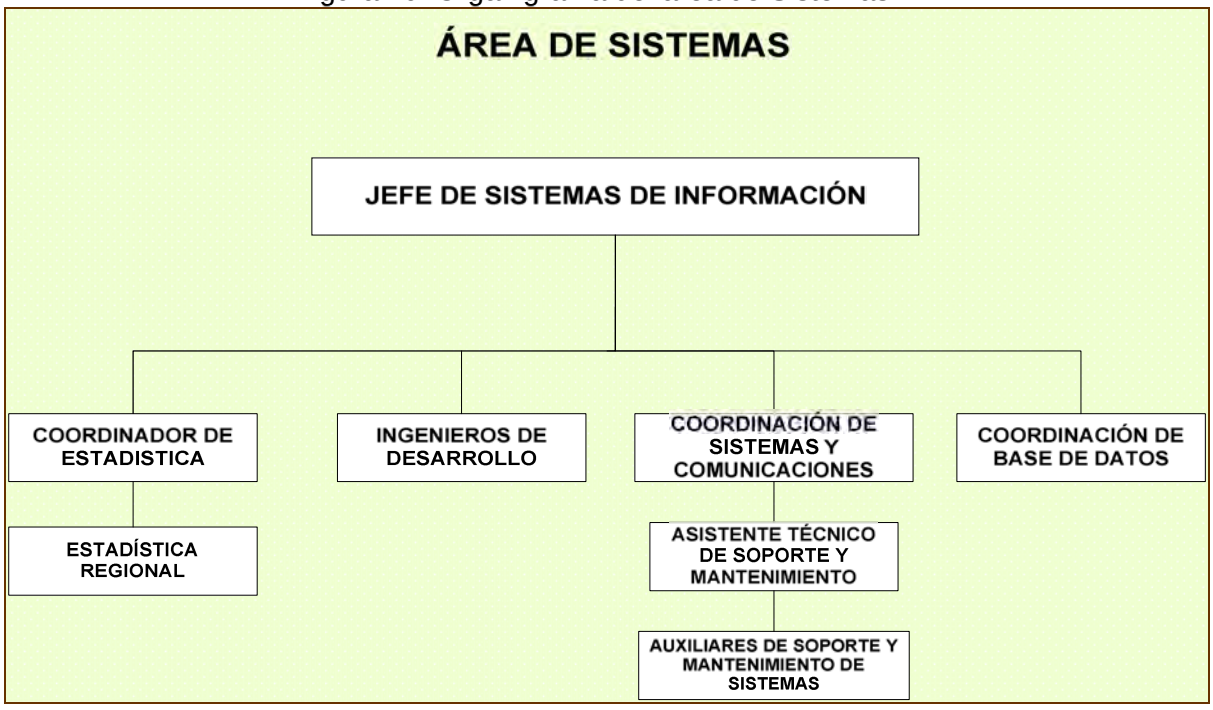
Organigrama zonal sur: el municipio de Ipiales, tomado como central de los municipios aledaños, trabaja como zonal de 11 municipios ubicados al sur de Nariño (Figura 9), así:

Figura 9: Organigrama zonal sur



Organigrama del área de sistemas. Aprobación**:** según resolución de gerencia general 009 de 2009 (figura 10).

Figura 10: Organigrama del área de Sistemas



Área de sistemas

El área de sistemas de Emssanar es un organismo que depende de la Gerencia Administrativa y Financiera, constituido como un espacio encargado de la administración de los sistemas y soporte centralizados, el objetivo de esta Área es la organización, control y automatización de la información corporativa. Dentro de las actividades que se desarrollan en el área de sistemas corresponde a la administración de los sistemas operativos con el objetivo de garantizar la continuidad del funcionamiento de las maquinas y del software al máximo rendimiento y facilitar su utilización a todas las dependencias de la empresa en general. Dentro de lo que concierne a las funciones de la coordinación de Sistemas y Comunicaciones lo que tiene que ver con el diseño, la implementación y el mantenimiento de los elementos que constituyen la infraestructura informática de la empresa, entendiendo como tal los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la empresa en general los servicios informáticos necesarios para desarrollar sus actividades

Dentro de las actividades se desarrollan tareas que sirven de control para el funcionamiento de los sistemas, están:

- Mantenimiento de los equipos, detección y resolución de averías.
- Sintonía del sistema operativo y optimización del rendimiento.
- Gestión de cuentas de usuario y asignación de recursos a las mismas.
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.

- Evaluación de necesidades de recursos (memoria, discos, unidad central) y provisión de los mismos en su caso.
- Instalación y actualización de utilidades de software.
- Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento).
- Organización de otros servicios como copia de ficheros en cinta, impresión desde otros ordenadores en impresoras dependientes de estos equipos.
- Instalación y configuración de los ordenadores centrales.
- Altas y bajas de usuarios, altas y bajas de equipos de cómputo.
- Instalación y configuración de aplicaciones en los servidores.
- Administración de las listas de correo
- Copias de seguridad de los datos de los usuarios y recuperación de los mismos en caso de pérdida.
- Instalación, configuración y mantenimiento de servicios como correo electrónico, proxy Web, entre otros.
- Diseño y configuración y administración de la red que interconecta todos los edificios de la empresa (Red de Comunicación).
- Selección e instalación de sistemas informáticos. Definición de configuraciones tanto para servidores como para puestos de trabajo.
- Elección de sistemas operativos. Selección e instalación de Software.
- Administración de sistemas
- Área de gestión de bases de datos.
- Administración de bases de datos
- Explotación de la información contenida en las bases de datos. Exportación de la información a formatos manejables por aplicaciones ofimáticas
- Área de desarrollo: nuevos desarrollos: análisis, programación y documentación
- Mantenimiento de Aplicaciones: corrección de errores, adaptación de los programas a nuevas necesidades (nuevas normativas, cambios organizativos).
- Área de soporte a usuarios y mantenimiento de equipos
- Soporte de aplicaciones
- Ofimática
- Área de asesoramiento
- Apoyo técnico a la dirección y servicios-unidades.
- Elaboración de informes
- Reparación y mantenimiento de equipos
- Administración del servicio de web
- Consolidación de la estructura de los sitios web.
- Mantenimiento y administración de la red
- Seguridad en la red
- Administración de direcciones IP de la red interna (en constante crecimiento)
- Mantenimiento de servidores de web, mail, nombres de dominio, firewall, proxy y cualquier otro que el área pueda desarrollar.
- Configuración y monitoreo de las líneas telefónicas del servicio Dial Up.
- Instalación y actualización del software.
- Definición de políticas de usuario.
- Backups.
- Mantenimiento de los servicios de correo electrónico

- Atención y soporte a usuarios del servicio.
- Control de la seguridad y privacidad del servicio.
- Mantenimiento de las cuentas de correo
- Actualización de bases de datos de usuarios de correo electrónico.
- Mantenimiento de las listas de correo electrónico
- Altas y bajas de las listas de interés general.
- Atención telefónica
- Atención personal
- Atención por correo electrónico
- Soporte red interna y representantes de la misma.
- Capacitación
- Capacitación a cargo de empleados del área de comunicaciones soporte administrativo
- Administración del software del área de comunicaciones
- Administración del hardware del área de comunicaciones
- Pedido de insumos para el área de comunicaciones.
- Manejo de documentos internos que hacen a la organización interna del área.

2.2.8 Manual de funciones área de sistemas. Dentro de Emssanar existe un documento que describe los cargos y las funciones para cada persona que hace parte de Emssanar y para el caso del área de sistemas, tenemos lo siguiente:

Coordinador del área de sistemas

Nombre del Cargo: Jefe de Sistemas de Información
Área: Gerencia Administrativa y Financiera
Dependencia: Jefatura de Sistemas
Nivel: Profesional
Personal encargado: Harold Caicedo
Funciones: Propender por el adecuado funcionamiento y optimización de los sistemas de información y comunicación. Así:

Por seguridad y riesgo:

- ✓ Garantizar la integridad de los sistemas de información.
- ✓ Garantizar la conservación del software y hardware
- ✓ Implementar alternativas de solución frente a los problemas de infraestructura e información.
- ✓ Elaborar e implementar planes de contingencia.
- ✓ Diseñar estrategias organizacionales para la captura, manejo y seguridad de la información.
- ✓ Analizar las potencialidades de riesgo a nivel del funcionamiento a nivel de hardware, software y comunicaciones.
- ✓ Diseñar e implementar estrategias para disminuir el riesgo en el manejo de la información organizacional.
- ✓ Analizar los conductos de transmisión de la información.

Por materiales, maquinaria y equipos:

- Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- Mantener en buen estado los equipos confiados a su responsabilidad.

Por información y documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Informar y orientar con criterios de calidad, oportunidad y veracidad a los usuarios interno y externo) que requieran el servicio.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Estadístico regional

Nombre del Cargo: Estadístico regional
Área: Gerencia administrativa y financiera
Dependencia: Jefatura de sistemas
Nivel: Profesional
Personal encargado: Ángela Constanza Hidalgo Erazo
Funciones: encargada proceso y secuencia de la seguridad y riesgo, contratación-afiliación y registro, atención con enfoque de riesgos. Así:

- ✓ Realizar el análisis de la información registrada en la ficha FIES (Ficha Inicial del Estado de Salud), previamente diligenciada en el momento de la entrega de carnets.
- ✓ Realizar para posterior reporte del análisis de la información de la ficha FIES a la Gerencia de Salud.
- ✓ Determinar el perfil de riesgo a través de la caracterización del territorio, caracterización de la población afiliada y diagnostico epidemiológico y formulación de los indicadores básicos en salud.
- ✓ Administrar la información estadística empresarial
- ✓ Realizar el análisis estadístico de la información
- ✓ Elaborar copias de seguridad de la información

Por Materiales, Maquinaria y equipos:

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.
- ✓ Responder por las herramientas para el mantenimiento preventivo y correctivo de los equipos de cómputo.

Por información y documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Ingeniero de desarrollo

Nombre del Cargo: Ingeniero de desarrollo
Área: Gerencia Administrativa y financiera
Dependencia: Jefatura de sistemas
Nivel: Profesional
Personal encargado: Mónica Cristina Girón Cerón - Jairo Fernando Obando Guanaran.
Funciones: encargada de proveer soluciones automatizadas que se ajusten a las necesidades especificas de la organización. Con las siguientes funciones en cuanto a seguridad y riesgo:

- ✓ Generar herramientas automatizadas (programas), que garanticen el control, la evaluación y el seguimiento del procesamiento e ingreso de la información.
- ✓ Identificar puntos de control en el procesamiento de la información.
- ✓ Eliminar los puntos de posible riesgo en pérdida o adulteramiento de la información organizacional.
- ✓ Proveer elementos para el seguimiento y evaluación de información que ingresa en el sistema.
- ✓ Identificar puntos de medición de tiempo en el procesamiento de la información.
- ✓ Determinar los conductos de comunicación a nivel del sistema de información y transferencia de datos.

Por materiales, maquinaria y equipos:

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.

Por Información y Documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Coordinador sistemas y comunicaciones

Nombre del Cargo: Ingeniero de desarrollo
Área: Coordinador sistemas y comunicaciones
Dependencia: Jefatura de sistemas
Nivel: Profesional
Personal encargado: Andrés Yepez Trejos.
Funciones: Responder oportunamente a los requerimientos de: información, normativos externa e interna, sus funciones:

En seguridad y Riesgo:

- ✓ Generar reportes confiables como resultado del análisis y consolidación de la información empresarial.
- ✓ Generar reportes confiables de acuerdo al requerimiento normativo.
- ✓ Identificar posibles pérdidas de información como resultado de manipulación y desviación en los procesos o en el inadecuado funcionamiento de los sistemas de información.
- ✓ Capacitar al personal involucrado en el proceso de implementación de herramientas automatizadas.
- ✓ Seguimiento y monitoreo al proceso de implementación de herramientas automatizadas.
- ✓ Retroalimentación con el área de sistemas de las herramientas automatizadas implementadas.

Por materiales, maquinaria y equipo:

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.

Por información y documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Asistente de soporte y mantenimiento

Nombre del Cargo: Asistente de soporte y mantenimiento
Área: Gerencia administrativa y financiera
Dependencia: Jefatura de sistemas
Nivel: Tecnológico
Personal encargado del manejo de mantenimiento: Diego Bastidas
Funciones: Garantizar el soporte técnico a nivel de: equipos de cómputo, redes, ofimática, y programas de desarrollo interno. Así:

Por seguridad y riesgo:

- ✓ Realizar mantenimiento preventivo de los equipos de cómputo.
- ✓ Realizar mantenimiento correctivo de los equipos de cómputo.
- ✓ Revisión y adecuación de las instalaciones eléctricas reguladas.
- ✓ Seguimiento de los puntos de control preestablecidos en el área de sistemas.
- ✓ Brindar apoyo técnico en el manejo de los programas de desarrollo interno preestablecidos en la organización

Por materiales, maquinaria y equipo:

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.
- ✓ Responder por las herramientas para el mantenimiento preventivo y correctivo de los equipos de cómputo.

Por información y documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Por materiales, maquinaria y equipos:

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.

Por información y documentación:

- ✓ Responder por la seguridad de documentos a su cargo y adoptar mecanismos para su conservación, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Cumplimiento del los diferentes reglamentos, normas y manuales de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

Coordinador de base de datos

Nombre del Cargo: Coordinador de base de datos
Área: Sistemas
Dependencia: Jefatura de sistemas
Nivel: Tecnológico
Personal encargado del manejo de mantenimiento: Sonia Guadalupe Chacón Freire.
Funciones: Apoyar en el proceso de afiliación, registro y carnetización efectiva, así:

Administración de la base de datos

- ✓ Cargar diariamente la base de datos, consolidando la información de las dos regionales en el aplicativo sincroniza.
- ✓ Generar le reporte final que garantice la conformación de la base de datos única empresarial.
- ✓ Notificar al coordinador regional de afiliación y registro sobre las inconsistencias en la información de las bases de datos para que se establezcan los correctivos necesarios.
- ✓ Corregir las inconsistencias de las bases de datos en el caso de los afiliados inactivos.

Por materiales, maquinaria y equipos

- ✓ Conocer y operar correctamente los equipos necesarios para cumplimiento de los procesos del área.
- ✓ Mantener en buen estado los equipos confiados a su responsabilidad.

Por documentación e información

- ✓ Responder por la información de documentos a su cargo y adoptar mecanismos para su información, buen uso y evitar pérdida de los mismos.
- ✓ Guardar reserva de la información confidencial de la empresa.
- ✓ Copias de Seguridad
- ✓ En cuanto a usuarios: Informar y orientar con oportunidad y veracidad a los usuarios que requieran el servicio
- ✓ Cumplimiento del los diferentes reglamentos, manuales y normas de la empresa.
- ✓ Participar en los programas de desarrollo humano organizados por la Empresa.

2.3. ARCHIVO CORRIENTE

2.3.1 Diagramas de procesos del área de sistemas

Emssanar E.S.S es una entidad que trabaja día a día por ser una de las entidades de salud que brinde sus servicios de mayor y mejor calidad, así mismo es importante que esta entidad adelante un sistema de gestión de calidad en pro del desarrollo competitivo a nivel empresarial.

A continuación se representa los procesos más importantes del área de sistemas de Emssanar E.S.S, con el propósito de entender el funcionamiento de esta área.

Diagrama de general del proceso soporte y mantenimiento

El objetivo del proceso de soporte y mantenimiento es brindar apoyo y solución a la exigencia técnica, tecnológica y operativa generada por el cliente interno de la organización, en cuanto al estado de funcionamiento, manejo y necesidades de recursos informáticos y de comunicación; además velando por la seguridad y custodia de los recursos.

En la representación del proceso de soporte y mantenimiento se puede reconocer los pasos que se siguen en el momento de prestar y atender las solicitudes de los clientes internos de acuerdo a la necesidad que se presente (Figura 11), así:

Figura 11: Diagrama general del proceso de soporte y mantenimiento.

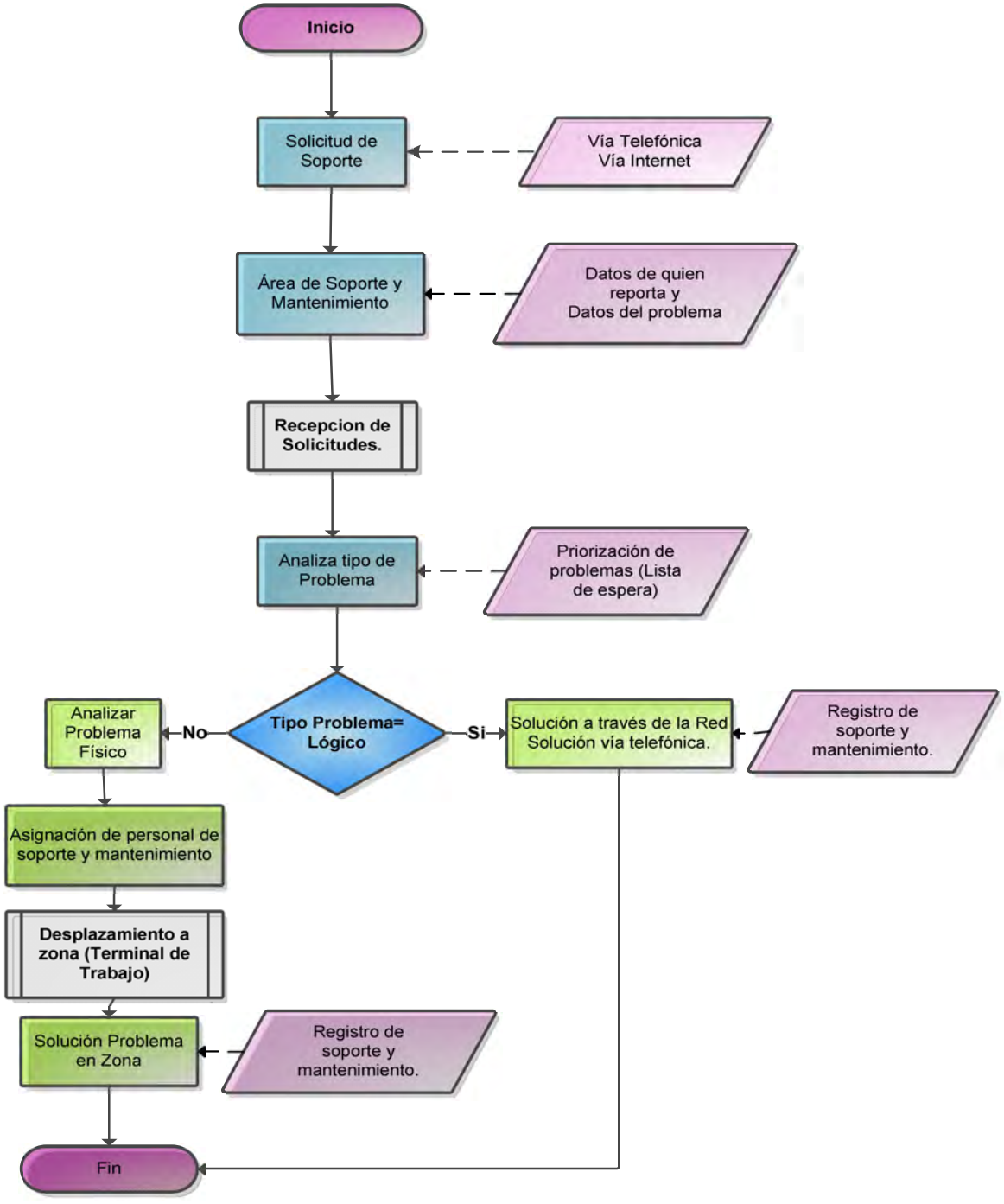


Diagrama de general del proceso solicitud de nuevo hardware

El Objetivo del proceso de Solicitud de Nuevo Hardware es identificar los requerimientos de infraestructura y soporte tecnológico de los clientes internos y externos de EMSSANAR E.S.S; necesarios para dar cumplimiento a los objetivos empresariales.

En la representación del proceso se puede reconocer los pasos que se siguen en el momento de solicitar cambio o nuevo hardware que los clientes internos deben seguir de acuerdo a la necesidad que se presente (Figura 12).

Figura 12: Diagrama general del proceso de solicitud de nuevo hardware.

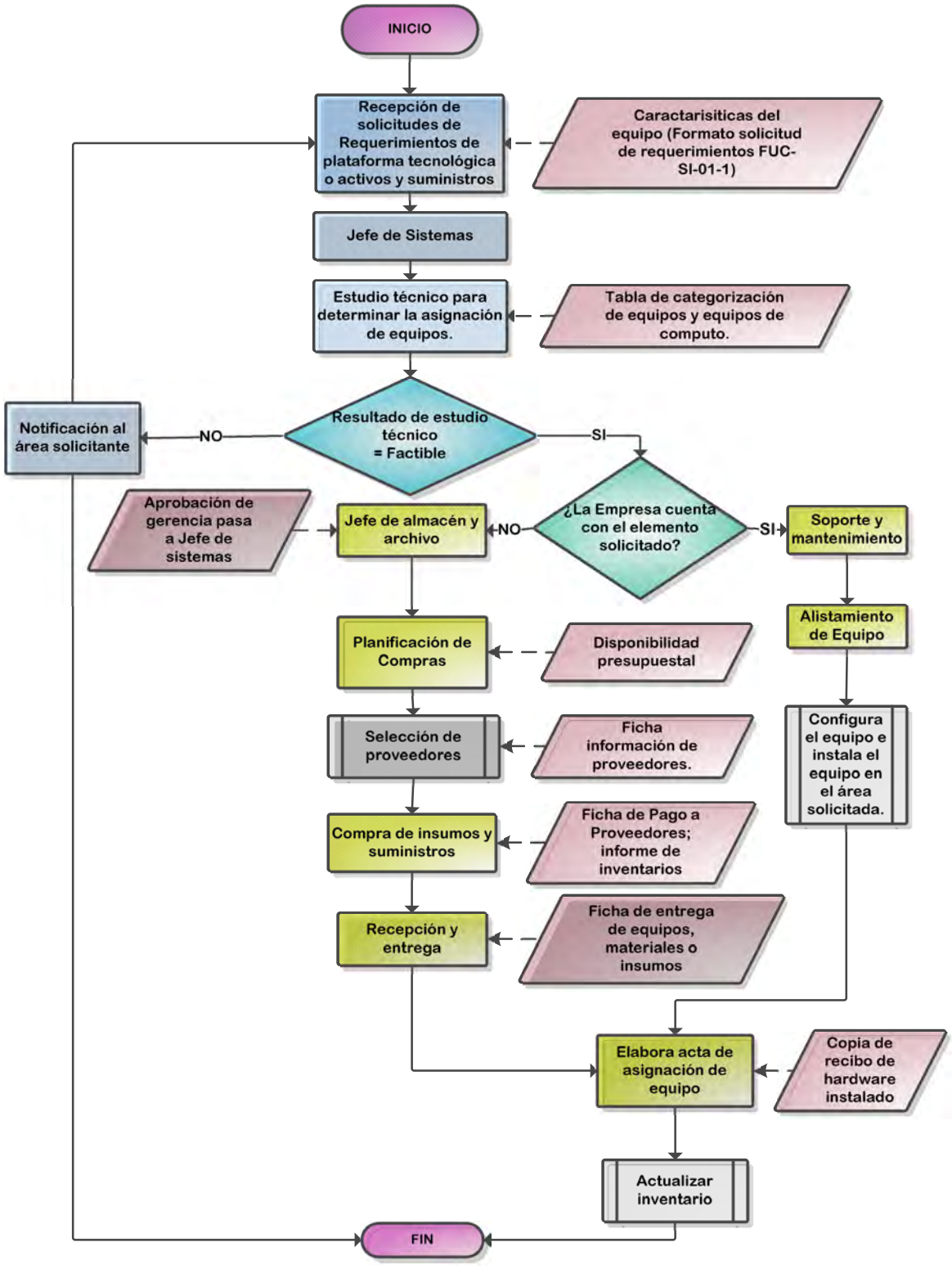


Diagrama general del proceso del nivel de obsolescencia

El objetivo del proceso de nivel de obsolescencia es propender por el óptimo funcionamiento de la infraestructura tecnológica y de comunicaciones para garantizar la disponibilidad del sistema de información.

En la representación del proceso se puede reconocer los pasos que se siguen en el momento de rotar o cambiar un equipo en el momento en que el personal de soporte y mantenimiento así lo requiera según las solicitudes de cambio o asignación de equipos del personal interno de acuerdo a la necesidad que se presente (Figura 13).

Figura 13: Diagrama general del proceso nivel de obsolescencia.

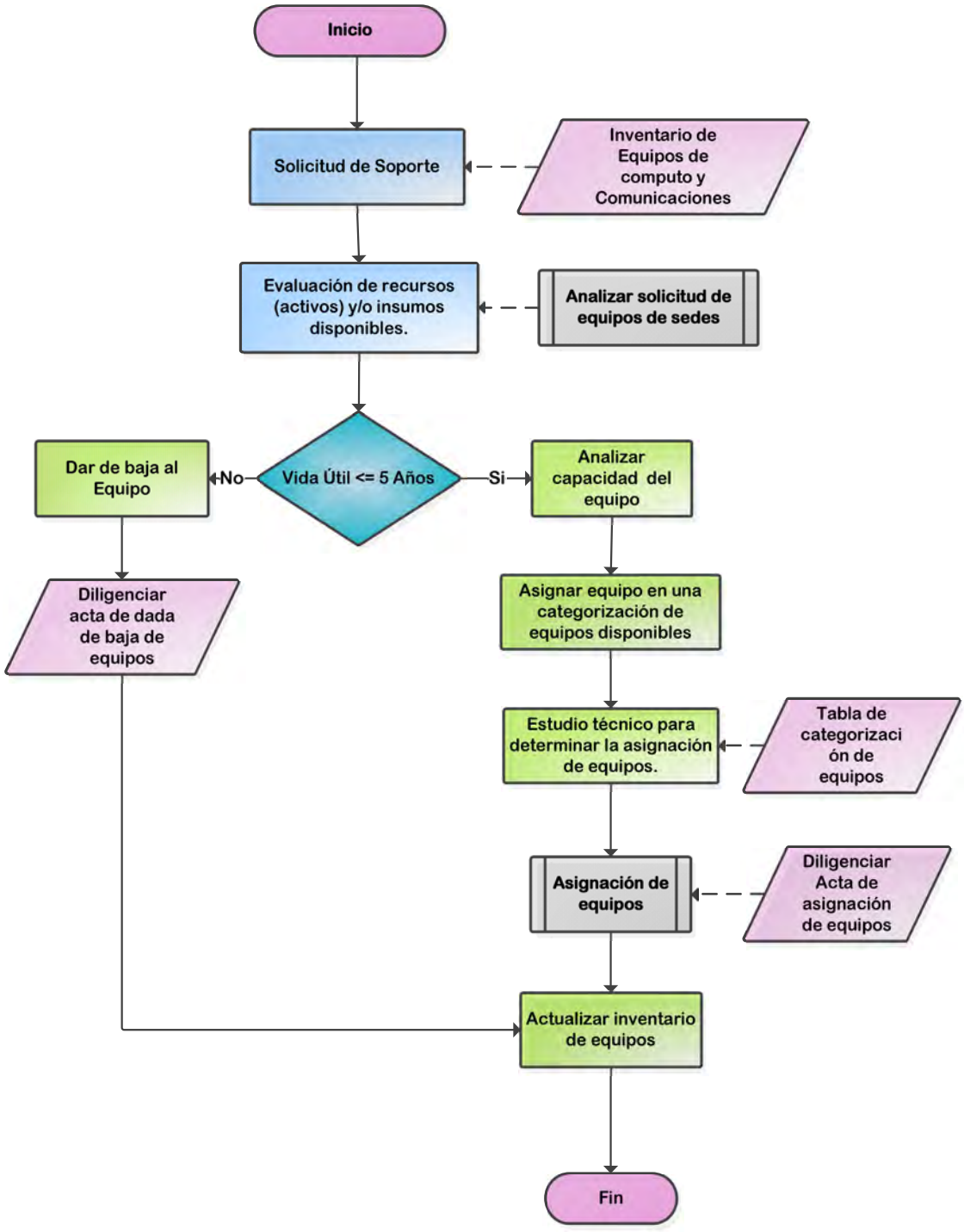


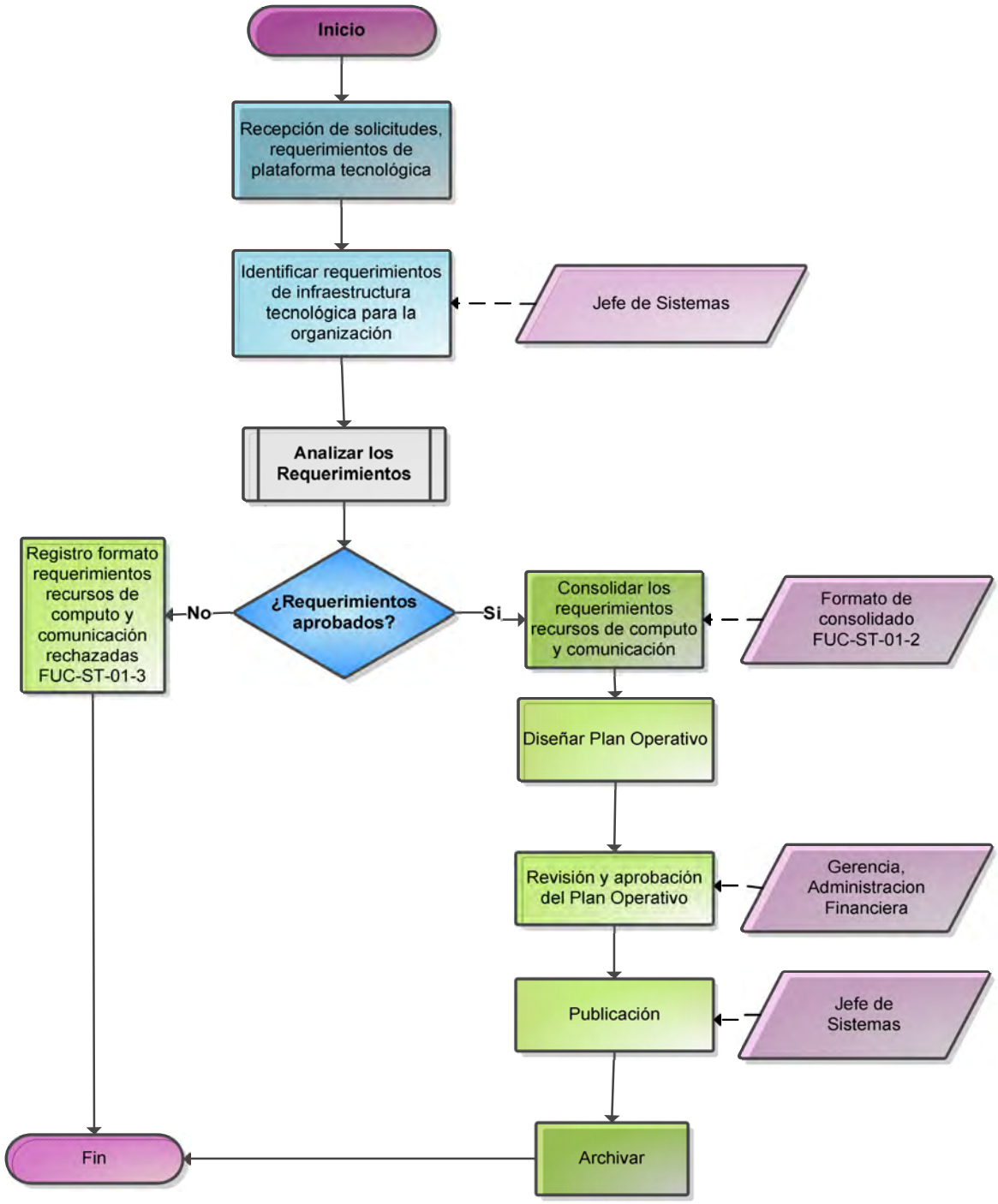
Diagrama general del proceso planificación de infraestructura y soporte tecnológico.

El objetivo es identificar los requerimientos de infraestructura y soporte tecnológico
En el tiempo establecido y así elaborar un Plan Operativo Anual de acuerdo a todas las solicitudes, análisis y evaluación de los requerimientos, así:

1) Requerimientos programados: aquellos requerimientos que los usuarios de la Plataforma Tecnológica presentan en el periodo comprendido entre el 1 de noviembre al 15 de diciembre de cada año para elaborar el POA del siguiente año.
2) Requerimientos no programados.

En la representación del proceso se puede reconocer los pasos que se siguen en el periodo establecido en que se debe diseñar el plan operativo (Figura 14)

Figura 14: Diagrama general del proceso planificación de infraestructura y soporte tecnológico.



2.3.2 Programa de auditoría. Es importante señalar y detallar el trabajo a realizarse, los procedimientos a emplearse en la auditoria informática en el área de sistemas e

indicadores de funcionamiento del hardware en la empresa solidaria de salud Emssanar E.S.S del departamento de Nariño, así, esta auditoría se ejecutara mediante la aplicación de la metodología COBIT (objetivos de control para la información y tecnologías afines), dentro del cual existen 4 dominios, de los cuales se aplicaran los siguientes:

2.3.2.1 Dominio: Planeación y organización (PO)

Encargado de definir las estrategias y tácticas de las Tecnologías de la Información que permitan contribuir al logro y cumplimiento de los objetivos empresariales, a través del uso óptimo y conocimiento de los recursos de TI, apropiados para las necesidades de la empresa. En la ejecución de la auditoria a realizarse se aplican los siguientes procesos:

PO3 Determinar la dirección tecnológica: encargado de evaluar la infraestructura tecnológica, La definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas. Se debe actualizar regularmente abarcando aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la empresa aproveche al máximo sus recursos tecnológicos.

- *PO3.1 Planeación de la dirección tecnológica:* analizar la tecnología existente en cuanto a la infraestructura de las comunicaciones y los servidores.
- *PO3.2 Plan de infraestructura tecnológica*: verificar que haya un plan de infraestructura tecnológica, evaluar planes de contingencia, evaluar procesos para la adquisición y la evolución de recursos tecnológicos.
- *PO3.3 Monitoreo de tendencias y regulaciones futuras:* debe existir un proceso para monitorear las directrices del funcionamiento de la infraestructura tecnológica.
- *PO3.4 Estándares tecnológicos:* evaluar si existen asesorías sobre el funcionamiento de la infraestructura, verificar si existen guías para la selección de la tecnología, medir el cumplimiento de estándares y directrices.

PO4 Definir los procesos, organización y relaciones de TI: Dentro del área de sistemas debe estar claro y definido el personal de la tecnología de la información, los roles, las funciones y responsabilidades, permitiendo el buen funcionamiento de servicios que satisfagan los objetivos de la empresa.

- *PO4.5 Estructura organizacional:* evaluar la estructura organizacional interna del área de sistemas que se ajuste a los requerimientos del personal.
- *PO4.6 Establecimiento de roles y responsabilidades:* evaluar el cumplimiento de los roles y las responsabilidades definidas para el personal de TI, en el área de sistemas (administradores de redes, administradores de servidores, supervisor de los indicadores de cumplimiento).
- *PO4.10 Supervisión:* revisar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades.
- *PO4.13 Personal clave de TI:* la empresa debe identificar al personal clave de TI, para realizar las diferentes tareas a ejecutar y esta debe conocer cuáles son sus tareas autorizadas.

PO9 Evaluar y administrar los riesgos de TI: Encargado de identificar, analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de la empresa, con el objetivo de asegurar el logro de los objetivos de TI.

- *PO9.1 Marco de trabajo de administración de riesgos*: el área de sistemas deberá establecer un marco de referencia de evaluación sistemática de riesgos. Deberá contener una evaluación regular de los riesgos de la parte física de las comunicaciones y servidores e indicadores de cumplimiento.
- *PO9.2 Establecimiento del contexto del riesgo:* establecer una metodología para la evaluación de riesgos, que garanticen resultados apropiados, bajo los criterios establecidos.
- *PO9.3 Identificación de eventos:* identificar riesgos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa), clasificar si son relevantes y en qué medida afectan los objetivos en este caso al área de sistemas y de la empresa.
- *PO9.4 Evaluación de riesgos de TI:* medir los riesgos, a través de la evaluación recurrente de la probabilidad e impacto de los riesgos identificados, usando métodos cuantitativos y cualitativos, que permitan obtener la magnitud del riesgo encontrado.
- *PO9.5 Respuesta a los riesgos:* definir un plan de acción contra riesgos, el proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos y así lograr mitigarlos.
- *PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos:* priorizar y planear las actividades de control y respuesta a la solución de riesgos encontrados, teniendo en cuenta también la parte económica de la solución de esta prioridad. monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

2.3.2.2 Dominio: Adquisición e implementación (AI)

Para llevar a cabo la estrategia TI, se debe identificar las soluciones, desarrollarlas y adquirirlas, así como implementarlas e integrarlas en la empresa, esto para garantizar que las soluciones satisfaga los objetivos de la empresa. De este dominio se aplicaran las siguientes actividades:

AI3 Adquirir y mantener infraestructura tecnológica: la empresa debe contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Contar con un plan operativo donde se garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.

- *AI3.1 Plan de adquisición de infraestructura tecnológica:* debe haber un plan que defina la adquisición, el mantenimiento de la infraestructura tecnológica, en este caso, en la parte física de las comunicaciones y de los servidores, un plan que satisfaga los requerimientos funcionales y técnicos de la empresa, se evaluara:
    - En cuanto a comunicaciones y a servidores, la capacidad, vida útil de los equipos tecnológicos, riesgos tecnológicos para la actualización de la tecnología al añadir capacidad técnica, proveedores de Red (Aprobados).

- *AI3.2 Protección y disponibilidad del recurso de infraestructura:* para proteger los recursos tecnológicos, la empresa debe implementar medidas de control interno, seguridad y adaptabilidad durante la configuración, integración y mantenimiento de la infraestructura como es en este caso el hardware de los equipos de comunicación y de los servidores, que garanticen la disponibilidad e integridad de los recursos tecnológicos. Se debe monitorear y evaluar el uso y las responsabilidades de la utilización que se dé a estos componentes de infraestructura.
- *AI3.3 Mantenimiento de la infraestructura:* la empresa debe desarrollar una estrategia de actualización y un plan de mantenimiento de la infraestructura, garantizar el control de los cambios de infraestructura tecnológica, incluir una revisión periódica contra las necesidades de la empresa, riesgos, identificar vulnerabilidades.
- AI3*.4 Ambiente de prueba de factibilidad:* evaluar la efectividad y eficacia de la infraestructura, sobre todo en los procesos de adquisición, funcionalidad, configuración de hardware, pruebas de desempeño, estructura de Red.

AI5 Adquirir recursos de TI: La empresa debe proveer recursos TI que así lo requiera de manera oportuna y rentable, incluyendo, personas, hardware y servicios, teniendo en cuenta la definición de procesos definidos de adquisición, selección de nuevos proveedores y estándares de adquisición de hardware.

- *AI5.1 Control de adquisición:* evaluar el procedimiento general de adquisiciones y estándares de infraestructura tecnológica, como son instalaciones, hardware (Comunicaciones y servidores).
- *AI5.2 Administración de contratos con proveedores:* revisar los contratos con proveedores en cuanto la adquisición de infraestructura tecnológica, debe existir en la empresa un procedimiento establecido para modificar y concluir contratos para todos los proveedores.
- *AI5.3 Selección de proveedores:* debe existir una lista de proveedores acreditados o un proceso de selección justa y viable de proveedores, que se ajuste a los requerimientos de la empresa.
- AI5.4 Adquisición de recursos de TI: se debe proteger y cumplir los intereses de la empresa en todos los contratos de adquisición de infraestructura tecnológica, incluyendo los derechos y obligaciones de las partes en los términos contractuales.

AI6 Administrar cambios: Para realizar algún cambio bien sea de hardware de comunicaciones o de servidores, relacionados con la infraestructura , debe existir un proceso que administre formalmente y controladamente dichos cambios, cada cambio debe seguir un proceso de recepción, evaluación, prioridad y autorización previo a la implantación, sin obviar la constatación o revisión después del cambio, esto con el fin de reducir riesgos que impacten negativamente la estabilidad o integridad del ambiente del buen funcionamiento de las comunicaciones y servidores.

- *AI6.1 Estándares y procedimientos para cambios:* evaluar que los procedimientos de cambio como es de infraestructura tecnológica se realicen bajo los criterios y estándares establecidos, según sea la solicitud y la prioridad de cada caso.
- *AI6.2 Evaluación de impacto, priorización y autorización:* evaluar el procedimiento de prioridades de solicitudes de cambios, pues debe haber una manera estructurada de los cambios en cuanto a impacto funcional de la empresa y así autorizarlo.

- *AI6.3 Cambios de emergencia:* la empresa debe tener establecido un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.
- *AI6.4 Seguimiento y reporte del estatus de cambio:* Se debe hacer un seguimiento a través de un reporte de las solicitudes de cambio, de solución y autorización.
- *AI6.5 Cierre y documentación del cambio:* Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

2.3.2.3 Dominio: dar soporte y servicio (DS)

Encargado de garantizar la entrega de los servicios requeridos por la empresa y se avalúan lo siguiente:

DS4 Garantizar la continuidad del servicio: es importante que dentro de la empresa se garantice la continuidad de los servicios de TI, para ello es importante desarrollar, mantener y probar planes de continuidad y así asegurar el mínimo impacto a la empresa en caso de una interrupción de servicios TI, esto se logra con el desarrollo y mantenimiento (mejorado) de los planes de contingencia de TI, con entrenamiento y pruebas de los planes de contingencia de TI y guardando copias de los planes de contingencia.

- *DS4.1 Marco de trabajo de continuidad de TI:* la empresa debe tener o definir la metodología de continuidad de TI, esto con el fin de ayudar a determinar la resistencia requerida de la infraestructura (comunicaciones y servidores) y de guiar el desarrollo de los planes de contingencia en caso de desastres, que permita por ejemplo evaluar el tiempo perdido por problemas de red, debido a interrupciones no planeadas, pero a la vez cuente con un plan de contingencia inmediato.
- *DS4.2 Planes de continuidad de TI:* la metodología de continuidad debe ser diseñado para reducir el impacto de un desastre, debe presentar diferentes alternativas de recuperación inmediata de los servicios, también debe cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.
- *DS4.3 Recursos críticos de TI:* revisar si se lleva un control de los planes de continuidad, de acuerdo al nivel de prioridad, asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias de la empresa y considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad.
- *DS4.4 Mantenimiento del plan de continuidad de TI:* se debe mantener el plan de continuidad activo, vigente y actualizado y que refleje de manera continúa los requerimientos actuales del departamento de sistemas de la empresa.
- *DS4.5 Pruebas del plan de continuidad de TI:* es importante que dentro de la empresa el plan de continuidad sea conocido por todas las partes interesadas, es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna. Hacer pruebas de continuidad de forma regular para asegurar que los procesos de TI pueden ser recuperados de forma efectiva y así probar que el plan es efectivo o sino corregir deficiencias en el plan, y así ejecutar un plan de acción para permitir que el plan permanezca aplicable.

- *DS4.6 Entrenamiento del plan de continuidad de TI*: la empresa debe asegurarse que todos las partes involucradas reciban sesiones de entrenamiento (Capacitaciones) de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS8 Administrar la mesa de servicio y los incidentes: responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de Emssanar, mediante una mesa de servicio bien diseñada y bien ejecutada. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.

- *DS8.1 Mesa de servicios*: establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI

DS12 Administración del ambiente físico: la empresa debe proporcionar y mantener un ambiente físico adecuado para proteger equipos, personal, como los activos de TI contra acceso, daño o robo, esto se logra con la Implementación de medidas de seguridad físicas y seleccionando y administrando las instalaciones.

- *DS12.1 Selección y diseño del centro de datos:* el área de sistemas debe definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia empresarial. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
- *DS12.2 Medidas de seguridad física:* evaluar las medidas de seguridad físicas alineadas con los requerimientos de la empresa. Las medidas deben incluir zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción de equipos. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.
- *DS12.3 Acceso físico:* la empresa debe definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.
- *DS12.4 Protección contra factores ambientales*: diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

- *DS12.5 Administración de instalaciones físicas:* se debe administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y de la empresa, las especificaciones del proveedor y los lineamientos de seguridad y salud.

2.3.2.4 Dominio: Monitorear y evaluar (ME)

Monitorear y evaluar los procesos correspondientes al hardware de comunicaciones y ores constantemente para asegurar el buen funcionamiento como también el desarrollo y cumplimiento de algunos Indicadores y que sigan las directrices implantadas por la empresa. Se aplicara lo siguiente:

ME1 Monitorear y evaluar el desempeño de TI: se evaluara el desempeño de TI en cuanto a los indicadores de funcionamiento en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio, verificar el cumplimiento con los objetivos de cada uno y que se hagan de acuerdo a la dirección y políticas establecidas, esto con el fin de implementar acciones de mejoramiento en el desempeño de estos.

- *ME1.1 Enfoque del monitoreo: S*e debe evaluar de los indicadores, el enfoque, el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios TI, monitorear la contribución de TI a la empresa.
- *ME1.2 Definición y recolección de datos de monitoreo: e*valuar si hay balance de objetivos de desempeño con los de la empresa como tal, definir referencias con que comparar los objetivos*,* e identificar datos disponibles a recolectar para medir los objetivos. Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.
- *ME1.3 Método de monitoreo*: monitorear que el área de sistemas de la empresa disponga de un método de monitoreo y control de seguimiento que garantice el desempeño de los indicadores.
- *ME1.4 Evaluación del desempeño:* comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.
- *ME1.5 Reportes al consejo directivo y a ejecutivos:* proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas de administración adecuadas.
- *ME1.6 Acciones correctivas:* identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: Revisión, negociación y establecimiento de respuestas de administración, asignación de responsabilidades por la corrección, rastreo de los resultados de las acciones comprometidas.

ME2 Monitorear y evaluar el control interno: monitorear de forma continua, comparar y mejorar el ambiente del área de sistemas de Emssanar, que se aplicara los siguientes:

- *ME2.1 Monitoreo del marco de trabajo de control interno:* deberá monitorear de forma continua, comparar y mejorar el ambiente de control de TI (infraestructura de la Red y de los equipos utilizados como servidores) y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.

- *ME2.6 Control interno para terceros:* evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicios externos cumplen con los requerimientos legales y regulatorios y obligaciones contractuales.

- *ME2.7 Acciones correctivas:* identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

2.3.3 Proceso de recolección de información y planteamiento de actividades

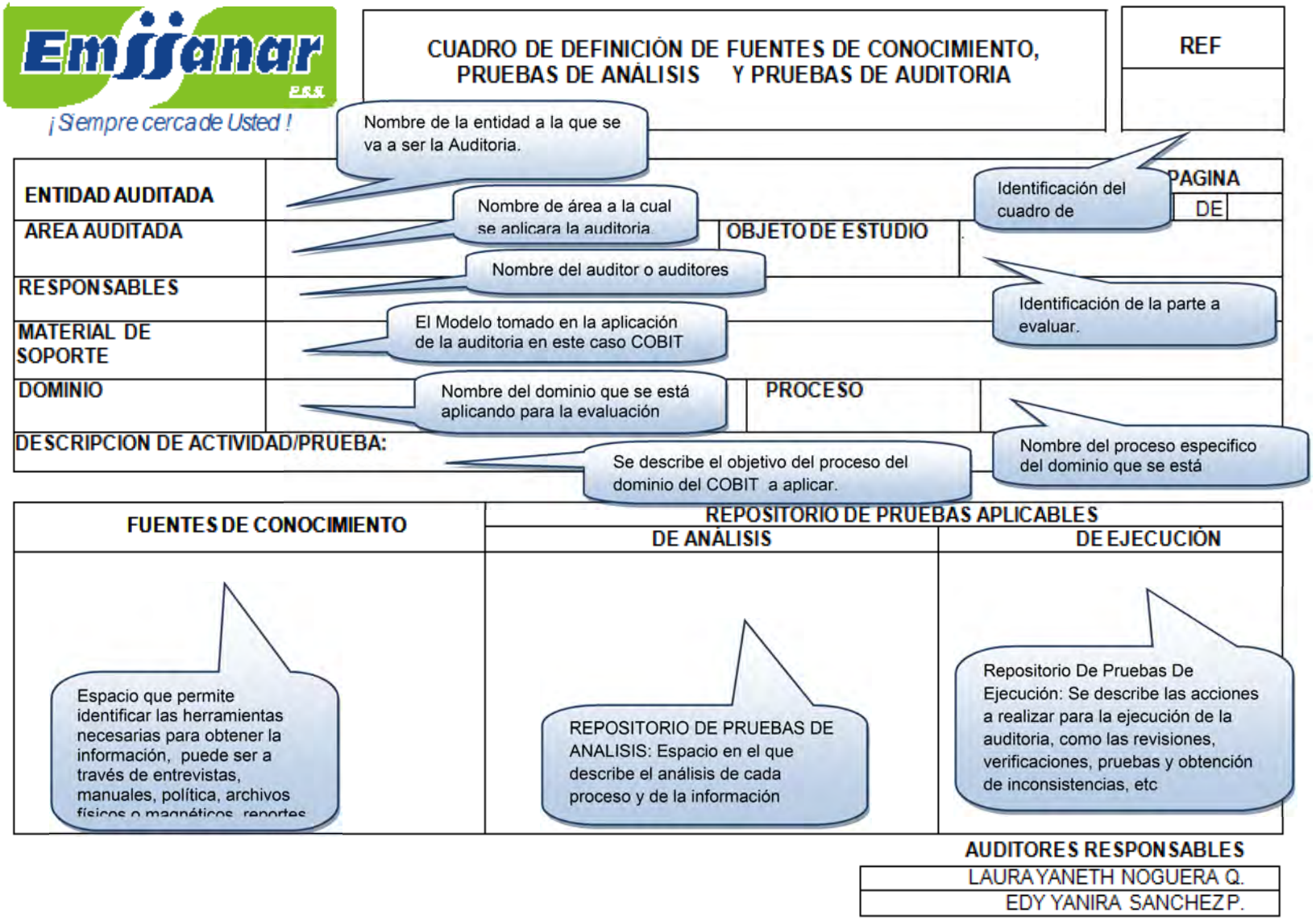
Para el desarrollo de la auditoria informática en el área de sistemas e indicadores de funcionamiento del hardware en la empresa solidaria de salud Emssanar E.S.S del departamento de Nariño, se utilizan los siguientes formatos de recolección de información:

Para dar comienzo a la auditoria, se realizaron diferentes entrevistas con el ingeniero Harold Caicedo, información que sirve para el reconocimiento de los diferentes procesos del área de sistemas de Emssanar, por tanto información clave para el desarrollo de este trabajo.

Cuadro de definición de fuente de conocimiento: permite obtener la información necesaria para establecer las fuentes de conocimiento, mediante la aplicación de los dominios del COBIT se evalúa la infraestructura física de comunicaciones, servidores e indicadores de la empresa, para luego realizar pruebas de análisis y de ejecución, permitiendo así obtener mayor claridad de la eficiencia y eficacia de los procesos del área de sistemas o en caso contrario identificar hallazgos con el objetivo de crear alternativas de solución.

Los cuadros de definición contienen el logo de la empresa a Auditar y los campos como la referencia, la entidad auditada, el objeto de estudios, entre otros, definidos en el siguiente formato (Figura 15), así:

Figura 15: Cuadro de definición de fuentes de conocimiento



Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar.

Con la aplicación del cuestionario cuantitativo se obtuvo el porcentaje de riesgo el cual se obtiene aplicando la siguiente fórmula:

$$\%\ de\ Riesgo = \frac{\text{Sumatoria de SI} * 100}{\text{Total Encuesta} - \text{Totales NA}}$$

Para determinar el nivel de riesgo total, se tuvo en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

Riesgo bajo: Deficiencias bajas en grado de importancia mayor, fáciles de solucionar a largo plazo.

*Riesgo medio: S*e debe tomar medidas de solución o mejora en un determinado periodo de tiempo.

Riesgo alto: se debe establecer soluciones inmediatas para reducir el riesgo sin afectar los objetivos del caso de estudio.

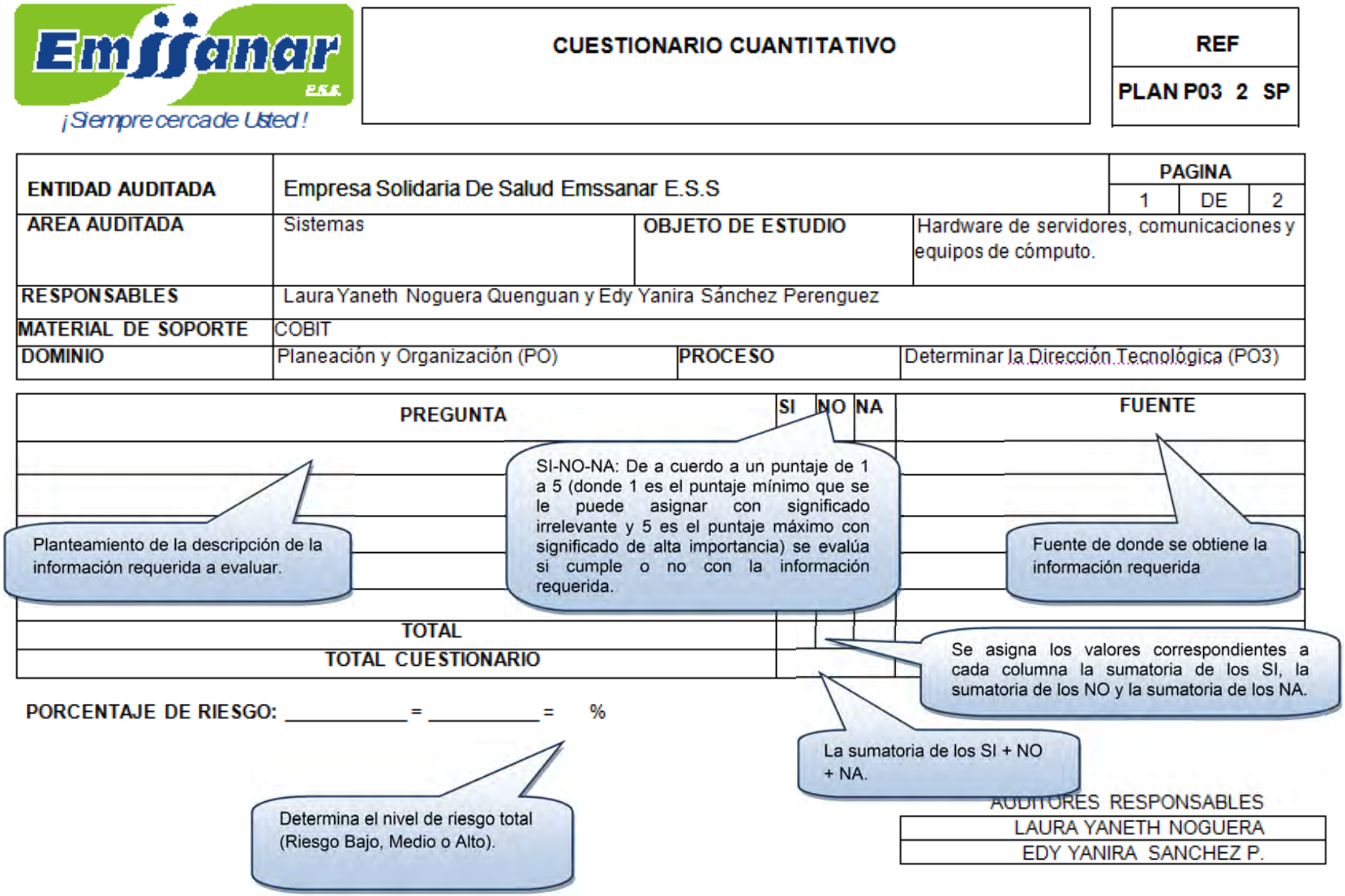
Entonces, se calcula así:

$$\%\ \text{de Riesgo Total} = 100 - \%\ \text{de Riesgo}$$

El resultado obtenido, permitió formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que este toma validez con la obtención de pruebas, que verifique los resultados de la encuesta.

Para ello se utilizo el siguiente formato (Figura 16):

Figura 16 Cuestionario cuantitativo



Entrevistas preguntas abiertas y preguntas cerradas: técnica utilizada para la recolección de información amplia que permita aclarar dudas que dejan los cuestionarios. Los formatos utilizados para hacer las entrevistas están ajustados al personal del área de Sistemas, al personal técnico y en general a todo el personal involucrado en el personal del área de tecnologías de la información y comunicación.

Se realizaron dos tipos de entrevistas:

Entrevistas con preguntas abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una.

Entrevistas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

Formatos presentados en las dos siguientes páginas, así:

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF**

ENTIDAD AUDITADA	Empresa Solidaria de Salud Emssanar ESS			**PAGINA** 1 DE 3	
ÁREA AUDITADA	Sistemas	**SISTEMA**	Riesgos de la parte física del establecimiento.		
OBJETIVO ENTREVISTA	Evaluar en qué condiciones se encuentra la parte física del establecimiento donde se encuentran ubicado el hardware (comunicaciones, servidores y equipos de computo).				

ENTREVISTADO	
CARGO	

1. ¿Existe un procedimiento para identificar los riesgos de seguridad física? ¿en qué consiste?

   _____

   _____

2. ¿De qué manera se identifican estos riesgos, quienes son los encargados de identificarlos?

   _____

   _____

3. ¿Existe un estudio de los riesgos encontrados?

   _____

   _____

4. ¿Qué procedimientos se aplican para el análisis y gestión de estos riesgos?

   _____

   _____

5. ¿Qué acciones se llevan a cabo para mitigar los riesgos en cuanto a seguridad física?

   _____

   _____

Nombre: _____
Firma: _____
Fecha de aplicación: _____

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores (Gestión de Riesgos)		

ENTREVISTADO	
CARGO	

PREGUNTA	**SI**	**NO**	**CUANTOS**	**OBSERVACION**

DATOS DEL ENTREVISTADO

NOMBRE	
CARGO	
FECHA DE APLICACION	

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

2.3.4 Análisis y evaluación riesgos preliminares

En el desarrollo de la auditoria se tiene en cuenta los 4 campos tomados como caso de estudio donde se hicieron las respectivas visitas y aplicación como tal de la auditoria. El proceso es el siguiente:

Como central: Se toma la sede principal que es la sede administrativa donde se encuentra la sede corporativa, es decir la sede de la regional Nariño – Putumayo. Teniendo en cuenta que en la ciudad de Pasto se encuentran distribuidas 7 sedes incluyendo la central, se definen nomenclaturas para la aplicación de las diferentes entrevistas y cuestionarios, así:

Tabla 1: Nombre de sedes y su nomenclatura

Nombre de la Sedes		Nomenclatura
Sede Principal		SP
CooEmssanar IPS		E.IPS
Laboratorio Clínico Emssanar		LAB
Fundación Emssanar		FE
Cresemillas	Servicio de Información y Atención al Usuario	SIAU
	Call Center (Centro de contactos)	CC
IPS Lorenzo		LZ
Como Zonal		
EPS Emssanar Zonal Ipiales.		IPI
Como Municipal		
Municipio de Córdoba. Atención al usuario Emssanar Córdoba		COR

Lista de riesgos encontrados

Emssanar sede principal (SP)

R1. No hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento de las comunicaciones.
R2. No hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento de los servidores.
R3. No hay Plan de seguridad de las comunicaciones (Acciones para mitigar riesgos)
R4. No hay diagrama de red de ninguna de las sedes.
R5. No existe documentación de la gestión de red de comunicaciones, se hace necesario crear un proceso para la gestión de red y si el software que se utiliza es suficiente.
R6. No hay hojas de vida de los servidores.

CooEmssanar IPS (E.IPS)

R1. Los funcionarios no conocen el manual de funciones
R2. A veces no se les informa de la fecha de mantenimiento de equipos.
R3. La red eléctrica no es segura por falta de ups y reguladores.

Laboratorio clínico Emssanar (LAB)

R1. No hay medidas de seguridad para el control de entradas ni salidas de la sede.
R2. No hay generadores de corriente si se fuese la energía.

Fundación Emssanar (FE)

R1. Internet con baja velocidad, limitación de accesos a internet.
R2. Se hace necesario mantenimiento más frecuente y actualización de vacunas, licencia permanente de antivirus. (Lentitud de equipos, etc.)
R3. Actualización de software. Los equipos tienen lo básico.
R4. No hay red eléctrica como tal para los computadores, se conectan directamente tampoco hay reguladores.
R5. Espacio limitado (espacio y movilidad limitada)
R6. No hay señales de evacuación (seguridad).

Cresemillas

R1: La seguridad del cuarto de comunicaciones o Rack no sigue las normas de seguridad establecidas en el estándar ANSI/TIA/EIA-569.

Servicio de información y atención al usuario (SIAU)

R1. Actualización de vacunas.
R2. Problemas en la máquina del digiturno
R3. Mantenimiento más frecuente
R4. No hay extintor.

Centro de contactos (CC)

R1. Deficiencia en cuanto al mantenimiento de los equipos y actualizaciones de vacunas.

IPS Lorenzo (solo hay un equipo) (LZ)

R1. La red de internet es lenta
R2. No se realiza previo aviso del mantenimiento de los equipos
R3. No se recibe rápida solución cuando se reporta un daño del equipo.
R4. No hay seguridad en esta sede (hace falta un vigilante)
R5. La instalación eléctrica y suministro de energía no es adecuada. (No hay polo a tierra)

EPS Emssanar zonal Ipiales (IPI)

R1. No hay planos de la red de datos.
R2. No hay extintor.
R3. Ubicación inadecuada de los equipos de comunicaciones como modem, servidores y reguladores.
R4. El tendido de cable no se acoge a las normas (canaleta en el piso, cables sueltos, canaletas abiertas)

Atención al usuario Emssanar Córdoba (Hay un solo equipo) (COR)

R1. En la oficina de atención al usuario no hay extintor.
R2. El cableado de red no es el adecuado, hay cables sueltos.

2.3.5 Valoración de riesgo. Teniendo en cuenta los riesgos encontrados, se toman los riesgos que para la empresa y según el caso de estudio tienen mayor importancia, de acuerdo a lo anterior se realiza la valoración de los riesgos teniendo en cuenta la probabilidad de ocurrencia y el impacto del riesgo dentro de lo que es Hardware de Comunicaciones, Servidores, equipos de Computo e Indicadores de funcionamiento de Emssanar ESS. En la siguiente tabla (Tabla 2) se unen los riesgos encontrados en las diferentes sedes, de acuerdo al caso de estudio del proyecto, se valora los riesgos y se clasifican dentro de los dominios del COBIT a los cuales corresponda según previo análisis, quedando definidos los riesgos así:

Tabla 2: Listado de riesgos

N. RIESGO	RIESGO	PROBABILIDAD			IMPACTO			DOMINIO
		B	M	A	B	M	A	
	Aseguramiento físico y eléctrico de los equipos de cómputo, los servidores y las comunicaciones.							
R1	En Emssanar ESS**,** el plan de contingencia en caso de que el hardware no funcione no está documentado. (SP)			X	X			(PO3)
R2	En Emssanar ESS no hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones. (SP)**.**			X			X	(PO9)
R3	No hay planos de red de datos de todas las sedes.			X			X	(AI3)
R4	En Emssanar ESS no existe documentación de la Gestión de red de comunicaciones. (SP)			X			X	(AI3)
R5	En Emssanar ESS, en cuanto a las condiciones físicas el espacio donde se encuentran ubicados los servidores no está bien adecuado y en la Fundación Emssanar el espacio donde se encuentran ubicados los equipos de computo es limitado no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura, posición de las columnas). (SP, FE).		X			X		(DS12)
R6	Ubicación inadecuada de los equipos de comunicación (Modem, Servidor, Patch panel). (IPI).			X		X		(DS12)
R7	En Cresemillas, la seguridad del cuarto de comunicaciones o Rack no sigue las normas de seguridad establecidas en el estándar ANSI/TIA/EIA-569. (CRE).			X		X		(DS12)
	Mantenimiento de equipos de cómputo, servidores, equipos de comunicación y red eléctrica.							
R8	Internet con baja velocidad, bloqueo y limitación de accesos a internet. (FE) y (LZ).		X			X		(PO9)
R9	En las sedes Fundación Emssanar y en el Centro de Contactos existe deficiencia en		X			X		(PO9)

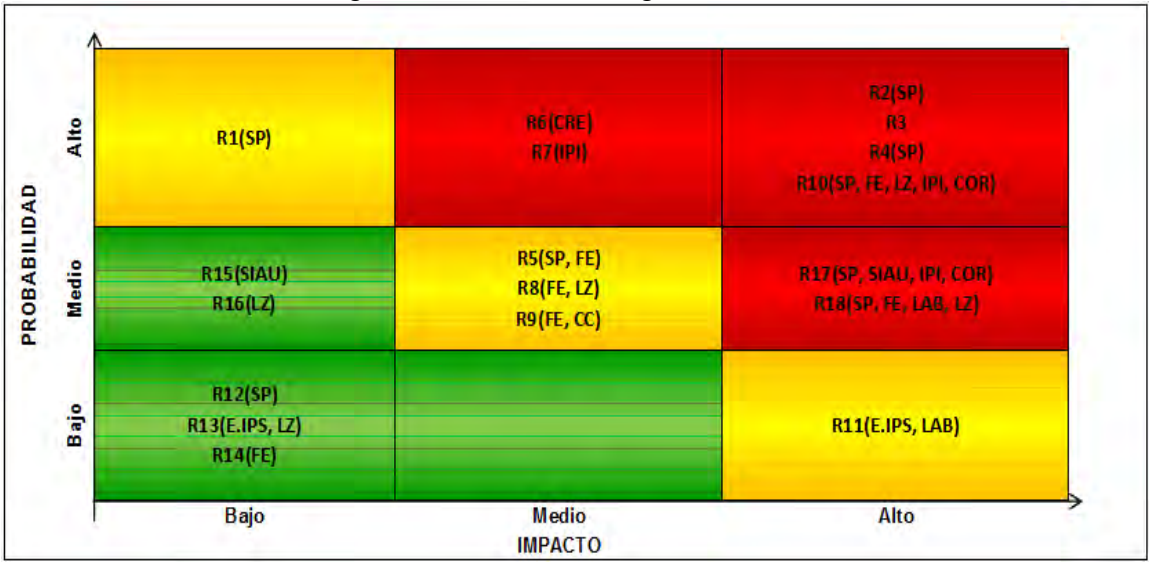
	cuanto al mantenimiento de los equipos y actualizaciones de vacunas. (FE, CC)							
N. RIESGO	**RIESGO**	**PROBABILIDAD**			**IMPACTO**			**DOMINIO**
		B	**M**	**A**	**B**	**M**	**A**	
R10	- En Emssanar ESS, el diagrama de Red Eléctrica no está actualizado. (SP) - En la Fundación Emssanar no hay red eléctrica segura, los computadores, se conectan directamente tampoco hay suficientes reguladores. (FE) - En la sede IPS Lorenzo la instalación eléctrica y suministro de energía no es adecuada. (No hay polo a tierra). (LZ) - En la sede EPS Emssanar Zonal Ipiales, el tendido de cable no se acoge a las normas EIA/TIA-568. (Canaleta en el piso, cables sueltos, canaletas abiertas). (IPI)			X			X	(DS12)
R11	- En la sede CooEmssanar IPS la red eléctrica no es segura por falta de UPS y reguladores. (E.IPS) - En la sede Laboratorio Clínico Emssanar No hay generadores de corriente si se fuese la energía. (LAB)	X					X	(DS12)
R12	No hay hojas de vida de los servidores.(SP)	X			X			(AI3)
R13	A veces no se les informa de la fecha de mantenimiento de equipos. (E.IPS, LZ)	X			X			(AI3)
R14	Actualización de software. Los equipos tienen lo básico.(FE)	X			X			(PO9)
R15	Problemas en la maquina del digiturno. (SIAU)		X		X			(AI3)
R16	No se recibe rápida solución cuando se reporta un daño del equipo. (LZ)		X		X			(AI3)
	Seguridad física de las instalaciones							
R17	- En Emssanar ESS, el espacio donde se encuentran ubicados los servidores no cuenta con materiales incombustibles (Pintura de las paredes, suelo, techo, mesas, etc). (SP). - En la sede Principal, no existe protección contra incendios ni otros peligros físicos que puedan afectar el espacio donde se encuentran ubicados los servidores. (SP). - En las sedes SIAU Y EPS Emssanar zonal Ipiales y en Atención al Usuario Emssanar Córdoba no hay extintor.		X				X	(DS12)

	(SIAU, IPI, COR)							

N. RIESGO	RIESGO	PROBABILIDAD			IMPACTO			DOMINIO
		B	M	A	B	M	A	
R18	- En Emssanar ESS, no existen sistemas de alarmas, ni cámaras de seguridad, ni detección de movimiento. (SP) - En la sede Fundación Emssanar no hay señales de evacuación. (FE) - En las sedes Laboratorio Clínico Emssanar y en la IPS Lorenzo no hay seguridad de vigilancia. (LAB, LZ)		X				X	(DS12)

Matriz de riesgos encontrados: Los riesgos encontrados durante la aplicación de la auditoria a traves de visitas, cuestionarios y entrevistas, se aplican dentro de la matriz de probabilidad e impacto donde se clasifican los riesgos de menor y mayor probabilidad e impacto, dando como resultado los sig:

Figura 17: Matriz de riesgos encontrados



De acuerdo al resultado mostrados en la anterior grafica (Figura 17), se toman los riesgos moderados (color amarillo) y riesgos altos (color rojo) como hallazgos encontrados durante la auditoria, por ser los de mayor probabilidad de ocurrencia y mayor impacto, los riesgos de color verde por ser de menor riesgo seran tomados como recomendaciones.

2.3.6 Técnicas y herramientas utilizadas

Se realizan los cuadros de deficion, cuestionarios y entrevistas aplicadas en la ejecucion de la auditoría.

Cuadros de definicion aplicados a la auditoria

De acuerdo al analisis del COBIT se aplican los procesos y de acuerdo al tipo de auditoria que se esta aplicando en el area de sistemas de Emssanar, se describen los cuadros de definicion, asi:

Emssanar E.S.S. ¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	REF PLAN PO3-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Determinar la Dirección **T**ecnológica (PO3)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Busca actualizar regularmente aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la empresa aproveche al máximo sus recursos tecnológicos.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al funcionario encargado del área de sistemas de Emssanar EPS de Pasto. • Entrevista al Coordinador de Sistemas y de Comunicaciones. • Entrevista a Asistente de Soporte y Mantenimiento. • Manual de Mantenimiento preventivo y Correctivo • Manual de Procedimientos Asistentes de Soporte y Mantenimiento. • Arquitectura de Red. • Instructivo Planes de Contingencia.	• Analizar la estructura y organización de la empresa • Analizar el Manual de Mantenimiento preventivo y Correctivo • Analizar el Manual de Procedimientos Asistentes de Soporte Y Mantenimiento. • Analizar la Arquitectura de Red (Diagramas, infraestructura, tipos de Red, topología de red). • Analizar las políticas de seguridad en caso de desastres de la Red. • Analizar las políticas o Manual de Asignación de Equipos, analizar el cumplimiento del procedimiento a seguir para cambios y reposiciones de equipos.	• Revisión detallada de los manuales de mantenimiento y Procedimientos. • Revisión detallada de la Arquitectura de red, de las políticas y aplicación de normas, • Revisión detallada de los planes de contingencia, el cumplimento de estas, el conocimiento de estos por el personal. • Revisión detallada de las directrices a seguir para la asignación de equipos.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	REF PLAN PO3-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.		**PAGINA**	**2 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
ATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Determinar la Dirección **T**ecnológica (PO3)	
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Busca actualizar regularmente aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la empresa aproveche al máximo sus recursos tecnológicos.				

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Instructivo Asignación de Equipos. • Estándares y Directrices de las comunicaciones. • Plan de infraestructura tecnológico • Soluciones tecnológicas	• Analizar el plan de infraestructura tecnológico. • Analizar soluciones tecnológicas existentes en la empresa.	• Revisar detalladamente el plan de infraestructura tecnológico. • Revisar soluciones tecnológicas

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.
EDY YANIRA SANCHEZ P.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	REF PLAN PO4-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la organización y las relaciones de TI (PO4)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Busca definir el personal de la tecnología de la información, los roles, las funciones y responsabilidades, permitiendo el buen funcionamiento de servicios que satisfagan los objetivos del área de Sistemas en concordancia con los de la empresa.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al funcionario encargado del área de sistemas. • Estructura organizacional del Área de Sistemas. • Entrevista con el funcionario encargado de realizar la actualización y el seguimiento a los indicadores. • Manual de funciones del personal de Emssanar EPS relacionado con el hardware de los servidores y las comunicaciones e indicadores. • Entrevista al funcionario que ejerce el rol de administrador del hardware (servidores, y comunicaciones)	• Analizar el manual de funciones del personal del área de sistemas. • Analizar la estructura y organización del área de sistemas. • Analizar los roles y responsabilidades del personal encargado de los servidores y las comunicaciones.	• Revisión detallada para evaluar la estructura organizacional del área de sistemas, asignación de responsabilidades y evaluar personal encargado del manejo de los recursos de las TI, identificando las personas claves del manejo de las comunicaciones. • Evaluar el procedimiento de contratación del personal del área de sistemas que tengan funciones relacionadas con los servidores y las comunicaciones e indicadores.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	REF PLAN PO4-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**2 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la organización y las relaciones de TI (PO4)		

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Busca definir el personal de la tecnología de la información, los roles, las funciones y responsabilidades, permitiendo el buen funcionamiento de servicios que satisfagan los objetivos del área de Sistemas en concordancia con los de la empresa.

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al funcionario encargado de realizar el seguimiento y actualización de los indicadores. • Políticas y procedimientos utilizados para determinar los requerimientos de asignación de personal de TI. • Descripción de roles y responsabilidades del personal encargado de operar el hardware de los servidores, las comunicaciones e indicadores.		• Una revisión detallada de las aptitudes del personal, las funciones y responsabilidades asignadas y separación de funciones. • Evaluar las actividades descritas en el manual de funciones y comparar con las actividades realizadas.

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.

EDY YANIRA SANCHEZ P.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN PO9-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 **DE** **2**	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargado de identificar, analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de la empresa, con el objetivo de asegurar el logro de los objetivos de TI, en este caso con la estabilidad y funcionamiento de las comunicaciones.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el Coordinador del hardware de las comunicaciones y los servidores. • Descripción de la evaluación de los riesgos de la parte física de las comunicaciones y los servidores. • Documento de la metodología para la evaluación de Riesgos. • Plan de Acción contra Riesgos • Políticas y procedimientos relacionados con la evaluación y gestión de riesgos relacionados con la parte física de los servidores y las comunicaciones.	• Analizar la evaluación de Riesgos. • Analizar el documento de la metodología de evaluación de Riesgos, identificar la medición de los riesgos, nivel de relevancia, etc. • Analizar el plan de Acción contra riesgos, identificar estrategias para evitar, reducir o mitigar el riesgo según sea conveniente, para tener impacto en las comunicaciones. • Analizar las políticas y procedimientos relacionados con la evaluación y gestión de riesgos relacionados con la parte física de los servidores y las comunicaciones	• Revisión detallada para evaluar los riesgos del hardware de las comunicaciones y los servidores, identificando la magnitud del riesgo y la priorización del riesgo, evaluando el impacto de este, la solución y el nivel de aceptación de estos. • Revisión detallada del plan de acción de riesgos, respuesta de solución de riesgos encontrados, monitorear el cumplimiento de la ejecución de los planes de acción.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN PO9-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**2 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargado de identificar, analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de la empresa, con el objetivo de asegurar el logro de los objetivos de TI, en este caso con la estabilidad y funcionamiento de las comunicaciones.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Plan de contingencia contra riesgos informáticos • Documentos de evaluación de riesgos.	• Análisis de los documentos de evaluación del riesgo del hardware de los servidores y las comunicaciones.	• Verificar si se han realizado simulacros de los planes de contingencia. • Una revisión detallada del enfoque de evaluación de riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual. • Revisión detallada de los planes de contingencia.

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.
EDY YANIRA SANCHEZ P.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN AI3-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica **(**AI3)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Satisfacer con los requerimientos de la empresa, el área de sistemas debe contar con un plan operativo donde se garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el funcionario encargado de realizar el mantenimiento preventivo y correctivo del hardware. • Entrevista al Coordinador de Sistemas y de Comunicaciones • Entrevista con el encargado del Mantenimiento del hardware de las comunicaciones y servidores. • Documento de Plan de Adquisición de Infraestructura Tecnológica. • Documento de contratos de adquisición	• Analizar los roles y las responsabilidades del personal encargado del manejo de los recursos tecnológicos. • Analizar el procedimiento general de adquisición y estándares de infraestructura tecnológica como son las instalaciones y el hardware de las comunicaciones y servidores.	• Revisión detallada del hardware en cuanto a: - Servidores - Red de comunicaciones - Equipos de comunicaciones - Instalaciones - cableado • Revisión de documentos relacionados con la adquisición e implementación de nuevo hardware.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN AI3-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				2	**DE** **2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica **(**AI3)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Satisfacer con los requerimientos de la empresa, el área de sistemas debe contar con un plan operativo donde se garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Documento de (Políticas de seguridad) protección y disponibilidad de recursos de infraestructura tecnológica. • Documento de lista de proveedores acreditados Planes de contingencia • Roles y responsabilidades del personal encargado de realizar el mantenimiento. • Entrevista con el funcionario encargado de aprobar la adquisición de nuevo hardware. • Plan de adquisición e implementación del hardware. • Plan de mantenimiento de hardware.	• Analizar las políticas y la aplicación de las normas relacionadas con la adquisición de la infraestructura tecnológica. • Analizar el plan de mantenimiento de la infraestructura de la tecnología. • Analizar el plan de contingencia	• Revisión detallada del plan de acción de riesgos, respuesta de solución de riesgos encontrados, monitorear el cumplimiento de la ejecución de los planes de acción. • Comparar los roles y responsabilidades estipuladas con las que en realidad realiza el personal. • Revisión detallada de las actividades de mantenimiento, para determinar si se está llevando a cabo un correcto mantenimiento.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN AI5-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 1 **DE** 2
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
ATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir recursos TI (AI5)	
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargado de proveer recursos TI según lo requiera la empresa de manera oportuna y rentable (Personal, hardware y servicios) teniendo en cuenta la definición de procesos definidos de adquisición, selección de nuevos proveedores y estándares de adquisición de hardware.				

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el jefe de sistemas encargado de autorizar las adquisiciones de hardware para servidores y comunicaciones. • Políticas y procedimientos estándares relacionados con la adquisición de nuevos recursos TI (hardware) • Políticas y procedimientos para modificar y concluir contratos para proveedores • Selección de proveedores acreditados	• Analizar la información de las últimas adquisiciones realizadas. • Analizar las políticas y procedimientos estándares relacionados con la adquisición de nuevos recursos TI (hardware) • Analizar las políticas y procedimientos para modificar y concluir contratos para proveedores • Analizar cómo se realizar la selección de los proveedores.	• Revisión detallada de la información de adquisición de recursos TI (hardware y personal) • Revisión detallada de la información relacionada con los procedimientos para modificar y concluir contratos para proveedores • Revisar la forma como se selecciona y como se realiza la contratación de proveedores. • Revisar el documento de contratos

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN AI6-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 **DE** **2**	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administrar Cambios (AI6)		

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargada de administrar cambios bien sea de hardware de comunicaciones o de servidores, relacionados con la infraestructura, cada cambio debe seguir un proceso de recepción, evaluación, prioridad y autorización previo a la implantación, esto con el fin de reducir riesgos que impacten negativamente la estabilidad o integridad del ambiente del buen funcionamiento de las comunicaciones y servidores.

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el jefe de sistemas, encargado de administrar formalmente y controladamente dichos cambios de hardware en cuanto a servidores y comunicaciones. • Procedimientos para evaluar cambios en la infraestructura tecnológica. • Procedimientos para priorizar solicitudes y aprobación de cambios de la infraestructura tecnológica. • Reportes de solicitudes de cambios	• Analizar el proceso que se lleva para realizar cambios de la infraestructura tecnológica. • Analizar los procedimientos para dar prioridad y aprobación de solicitudes de cambios. • Analizar los reportes de cambios de la infraestructura.	• Revisión detallada de la información de los cambios de la infraestructura tecnológica. • Revisión detallada de la información relacionada con los procedimientos para priorizar y aceptar los cambios. • Revisión detallada de los reportes de solicitudes de cambios.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS4-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.		**PAGINA**	**1 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
ATERIAL DE SOPORTE	COBIT			
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Garantizar la continuidad del servicio (DS4)	
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargado de garantizar la continuidad de los servicios de TI, para ello es importante desarrollar, mantener y probar planes de continuidad y así asegurar el mínimo impacto a la empresa en caso de una interrupción de servicios TI.				

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el Jefe de Sistemas • Metodología de continuidad de TI. • Plan de continuidad. • Control de los planes de continuidad. • Documento del mantenimiento del plan de continuidad. • Procedimientos para capacitar personal en caso de desastres y aplicar un plan de contingencia.	• Análisis la metodología de continuidad de servicios y así reducir impactos de desastres. • Analizar la actualización y el control de los planes de continuidad de los servicios. • Analizar que todas las partes involucradas reciban sesiones de entrenamiento respecto a los procesos, roles y responsabilidades en caso de un incidente o desastre.	• Revisión de la metodología de continuidad de los servicios TI. • Revisión detallada del plan de continuidad de los servicios TI. • Revisión de las funciones de la mesa de servicio donde se atienda y analice llamadas de incidentes reportados. • Revisión detallada del cumplimiento de los procedimientos de

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS8-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Administrar la mesa de servicios y los incidentes (DS8)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de Emssanar, mediante una mesa de servicio bien diseñada y bien ejecutada.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el jefe de sistemas. • Entrevista con el personal encargado de atender la mesa de servicios. • Políticas y procedimientos para dar solución a problemas de usuarios relacionados con servidores y comunicaciones. • Funciones de la mesa de servicios que atiende llamadas de incidentes reportados.	• Análisis de la información obtenida de los usuarios entrevistados con respecto a la mesa de servicios. • Analizar las políticas y los procedimientos que dan solución a problemas de usuarios relacionados con TI • Analizar las funciones de la mesa de servicios.	• Revisión detallada de los procedimientos para solucionar de manera oportuna y efectiva los problemas de los usuarios relacionados con servidores y comunicaciones. • Revisión de las funciones de la mesa de servicio donde se atienda y analice llamadas de incidentes reportados

Emssanar E.S.S. ¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS8-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**2 DE 2**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Administrar la mesa de servicios y los incidentes (DS8)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de Emssanar, mediante una mesa de servicio bien diseñada y bien ejecutada.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Políticas y procedimientos de monitoreo para clasificar y priorizar problemas.	• Analizar el monitoreo para clasificar y priorizar problemas.	• Revisión detallada de los procedimientos de monitoreo para clasificar y priorizar cualquier problema. • Medir la satisfacción de los usuarios con respecto a la calidad de la mesa de servicios.

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.
EDY YANIRA SANCHEZ P.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS12-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 3**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Administración de Instalaciones (DS12)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargada de mantener un ambiente físico adecuado para proteger equipos, personal, como los activos de TI contra acceso, daño o robo, tomando medidas de seguridad físicas.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al personal encargado de la seguridad física de las instalaciones. • Políticas y procedimientos para controlar el acceso físico a las instalaciones donde se encuentran los servidores y las redes de comunicaciones • Políticas y procedimientos para la protección de factores ambientales.	• Análisis de los controles para la entrada y salida a las instalaciones. • Análisis de las políticas y procedimientos para asegurar las instalaciones contra factores ambientales o naturales. • Analizar las pólizas de seguros del hardware de los equipos (servidores y comunicaciones).	• Revisión detallada la arquitectura de Red. • Revisión detallada de las instalaciones de Emssanar en cuanto a. - Acceso físico al edificio. - Red de comunicaciones. - Acceso a los servidores. - La estructura del edificio. - La seguridad contra incendios y desastres naturales. - Planes de evacuación del personal. - Revisiones de todos los seguros y bisagras.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS12-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**2 DE 3**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Administración de Instalaciones (DS12)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargada de mantener un ambiente físico adecuado para proteger equipos, personal, como los activos de TI contra acceso, daño o robo, tomando medidas de seguridad físicas.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Políticas y procedimientos para asegurar las instalaciones ante desastres ocasionados por la actuación humana. • Pólizas de seguros del hardware de servidores y comunicaciones. • Arquitectura de Red.	• Analizar las políticas y procedimientos para asegurar las instalaciones ante desastres ocasionados por la acción humana. • Analizar el diseño y la arquitectura de Red.	- Suministro de energía para el hardware. - Interconexión de redes y sistemas. - Acceso físico a las terminales de trabajo. - Localización física de las terminales de trabajo. - Instalaciones eléctricas. - Sistemas de ventilación en los centros de cómputo. - Llaves, cerraduras y gabinetes del centro de cómputo.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN DS12-1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 **DE** 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Administración de Instalaciones (DS12)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargada de mantener un ambiente físico adecuado para proteger equipos, personal, como los activos de TI contra acceso, daño o robo, tomando medidas de seguridad físicas.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
		- Instalación en el centro de cómputo de dispositivos de detección de humo, detección de calor y supresión de incendios. - Instalación de cámaras de seguridad. - Control de ventanas y visibilidad desde el exterior. - Sistemas de UPS. - Comprobación de la seguridad del cableado

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.
EDY YANIRA SANCHEZ P.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN ME1_1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 1**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y evaluar el desempeño de TI (ME1)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Encargado de evaluar el desempeño de TI en cuanto a los indicadores de funcionamiento en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio, verificar el cumplimiento con los objetivos de cada uno.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el personal encargado del manejo, control, actualización y cumplimiento de los indicadores. • Metodología de la evaluación de los indicadores. • Documento de los indicadores en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio. • Proceso del nivel de cumplimiento de los indicadores. • Reporte semestral de los indicadores de los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio.	• Analizar la metodología de la evaluación de los indicadores. • Analizar el documento de los indicadores en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio. • Analizar el proceso del nivel de cumplimiento de los indicadores. • Analizar el documento del Reporte semestral de los indicadores de los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio.	• Revisar detalladamente a metodología de evaluación de cumplimiento de los indicadores. • Revisar y verificar la información del documento de los indicadores en los noveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio. • Revisar el reporte semestral de los indicadores.

¡Siempre cerca de Usted !	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA**	**REF** PLAN ME2_1

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	**1 DE 1**
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
ATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y evaluar el control interno (ME2)		
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Monitorear y evaluar el control interno, proporcionando seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.					

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista con el funcionario encargado del realizar el control interno de Emssanar EPS. • Políticas y procedimiento relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física de los recursos Tecnológicos como hardware de servidores y comunicaciones.	• Analizar la información relacionada con TI dentro del control interno • Analizar las políticas y procedimientos de monitoreo de actividades de seguridad física de recursos TI	• Revisión detallada de los contenidos de TI dentro del control interno. • Revisión detallada de las políticas y procedimientos de monitoreo de actividades de seguridad física de recursos TI

AUDITORES RESPONSABLES

LAURA YANETH NOGUERA Q.
EDY YANIRA SANCHEZ P.

Cuestionarios y entrevistas aplicados en la auditoria

Dominio: Planeación y organización (PO)

- ✓ **PO3 Determinar la dirección tecnológica**

La información que se busca obtener con la aplicación del cuestionario está relacionada con datos del hardware de comunicaciones, servidores y equipos de cómputo.

Entrevista: se busca recolectar información con respecto a planes de infraestructura tecnológica, que confirmen respuestas del cuestionario, planes de contingencia, inventarios de equipos, etc.

- ✓ **PO4 Definir los procesos, organización y relaciones de TI**

Recolectar información concerniente a la definición del área de sistemas, es decir obtener datos de las funciones del personal de TI, planes de contingencia en caso de reemplazo de personal, políticas en cuanto a contratación de personal, etc.
Entrevista: confirmar la información suministrada por el cuestionario.

- ✓ **PO9 Evaluar y administrar los riesgos de TI**

Recolectar información concerniente al manejo de los riesgos de los recursos de hardware de equipos de TI.

Entrevista: confirmar información suministrada en el cuestionario en cuanto a identificar si existen controles para mitigar riesgos. También se realizo algunas entrevistas al personal de diferentes áreas de la sede principal y algunas sedes con el fin de evaluar el desempeño de los equipos que los usuarios operan.

¡Siempre cerca de Usted !	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN P03_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 1 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores, y Equipos de Cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Determinar la Dirección		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existe un plan de infraestructura tecnológica?				
2. El plan de infraestructura tecnológica contempla: • ¿Procesos de adquisición de recursos tecnológicos?				
• ¿Procesos de aprobación de adquisición de recursos tecnológicos?				
• ¿Estrategias de contingencia?				
3. ¿Se lleva un control y una actualización del plan de infraestructura?				
4. ¿Existe un inventario actualizado del hardware de comunicaciones?				
5. ¿Existe un inventario actualizado del hardware de servidores?				
6. ¿Existe un inventario actualizado del hardware de equipos de cómputo?				
7. ¿Existe un plan de rotación?				
8. ¿El proceso de rotación ayuda a dar un manejo apropiado a los equipos de cómputo				
9. ¿Existen planes de contingencia en caso de que el hardware no funcione?				
10. ¿Esos planes de contingencia están documentados?				
11. ¿Existe hardware adicional para reemplazar equipos que presenten fallas?				
12. ¿Existen hojas de vida de los servidores?				
13. ¿Existen hojas de vida de los equipos de cómputo?				
14. ¿Existe una persona encargada de vigilar el buen funcionamiento del hardware?				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT PO3_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			**PAGINA** 1 DE 1
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores	

ENTREVISTADO	ING. JESUS RECALDE
CARGO	Asistente de Soporte y Mantenimiento.

	SI	NO	OBSERVACION
1. ¿Existe un plan de infraestructura tecnológica?			
2. El plan de infraestructura tecnológica contempla: • ¿Procesos de adquisición de recursos tecnológicos?			
• ¿Procesos de aprobación de adquisición de nuevos recursos tecnológicos?			
• ¿Estrategias de contingencia?			
• ¿Este plan está documentado?			
3. ¿Se lleva un control y una actualización del plan de infraestructura?			
4. ¿Existe un inventario actualizado del hardware de comunicaciones?			
5. ¿Existe un inventario actualizado del hardware de			
6. ¿Existe un inventario actualizado del hardware de equipos de cómputo?			
7. ¿Existe un proceso de rotación?			
8. ¿El proceso de rotación ayuda a dar un uso apropiado a los equipos de cómputo existentes?			
9. ¿Existen planes de contingencia en caso de que el hardware no funcione?			
10. ¿Esos planes de contingencia están documentados?			
11. Estos planes de contingencia contienen: - ¿Objetivos claros para restaurar los servicio de forma rápida, eficiente y con el menor costo y pérdidas posibles?			
- ¿Pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del los servicios?			
- ¿Estrategias para la recuperación de desastres?			
12. ¿Existe hardware adicional para reemplazar equipos que presenten fallas?			
13. ¿Existen hojas de vida de los servidores?			
14. ¿Existen hojas de vida de los equipos de cómputo?			
15. ¿Existe una persona encargada de vigilar el buen funcionamiento del hardware?			

¡Siempre cerca de Usted !	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN O4 2 SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores, y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la organización y las relaciones de TI (PO4)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existe un manual de funciones para el personal encargado del manejo del hardware?				
2. El manual de funciones cumple con los siguientes requisitos: • ¿Existe una identificación completa (denominación, código, nivel, salario, etc.) del cargo a desempeñar?				
• ¿Existe la descripción de los diferentes perfiles (técnico, profesional, etc.) que debe cumplir cada uno de los funcionarios de TI?				
• ¿Existe una definición o descripción del cargo?				
• ¿Están claramente definidas las funciones que debe desempeñar el trabajador en los diferentes cargos?				
3. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de servidores?				
4. El manual de funciones para los usuarios que interactúan con el hardware de los servidores, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?				
• ¿Están definas las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan en cuanto al manejo y funcionamiento del hardware?				
• ¿Existe una descripción de los procesos que deben desempeñar los diferentes usuarios?				
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos, servicios, etc.) que debe cumplir el personal encargado del hardware?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN O4 2 SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 2 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores, y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la organización y las relaciones de TI (PO4)		

PREGUNTA	SI	NO	NA	FUENTE
5. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de comunicaciones?				
6. El manual de funciones para los usuarios que interactúan con el hardware de las comunicaciones, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?				
• ¿Están definas las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan en cuanto al funcionamiento del hardware?				
• ¿Existe una descripción de los procesos que deben desempeñar los diferentes usuarios?				
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos de la red, servicios de red, etc.) que debe cumplir el personal encargado del funcionamiento del hardware?				
7. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de los equipos de cómputo?				
8. El manual de funciones para los usuarios que interactúan con el hardware de los equipos de computo, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?				
• ¿Están definas las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan en cuanto al funcionamiento del hardware?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN O4 2 SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores, y Equipos de Computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la organización y las relaciones de TI (PO4)	

PREGUNTA	SI	NO	NA	FUENTE
• ¿Existe una descripción de los procesos que deben desempeñar los diferentes usuarios?				
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos, servicios, etc.) que debe cumplir el personal encargado del funcionamiento				
9. ¿Existen planes de contingencia para reemplazar a algunos funcionarios en caso de ausencia?				
10. El plan de contingencia para reemplazar a empleados cumple con los siguientes requisitos: • ¿Está documentado?				
• ¿Procedimientos para la contratación de personal de reemplazo?				
11. ¿Existen personas claves en la operación, administración y funcionamiento del hardware?				
12. ¿Existe personal indispensable que opere o administre el hardware?				
13. ¿Existen políticas y procedimientos para realizar la contratación de personal nuevo?				
14. ¿las políticas de contratación de personal nuevo, cumple con los siguientes requisitos: • ¿Cualquier persona que cumpla con los requisitos puede aspirar a los diferentes cargos?				
• ¿La selección se hace de un grupo de aspirantes que cumplan con los requisitos?				
• ¿Para la selección del personal de TI a contratar, se aplica el principio de la meritocracia?				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** ENT PO4_SP

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA**	1 DE 2
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores		

ENTREVISTADO	ING. JESUS RECALDE
CARGO	Asistente de Soporte y Mantenimiento.

PREGUNTA	SI	NO	OBSERVACION
1. ¿Existe un manual de funciones para el personal encargado del manejo del hardware?			
2. El manual de funciones cumple con los siguientes requisitos:			
• ¿Existe una identificación completa (denominación, código, nivel, salario, etc.) del cargo a desempeñar?			
• ¿Existe la descripción de los diferentes perfiles (técnico, profesional, etc.) que debe cumplir cada uno de los funcionarios de TI?			
• ¿Existe una definición o descripción del cargo?			
• ¿Están claramente definidas las funciones que debe desempeñar el trabajador en los diferentes cargos?			
3. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de servidores?			
4. El manual de funciones para los usuarios que interactúan con el hardware de los servidores, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?			
• ¿Están definidas las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan en cuanto al manejo y funcionamiento del hardware?			
• ¿Existe una descripción de los procesos que deben desempeñar los diferentes usuarios?			
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos, servicios, etc.) que debe cumplir el personal encargado del hardware?			
5. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de comunicaciones?			
6. El manual de funciones para los usuarios que interactúan con el hardware de las comunicaciones, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?			

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** ENT PO4_SP

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA**	2 DE 2
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores		

ENTREVISTADO	ING. JESUS RECALDE
CARGO	Asistente de Soporte y Mantenimiento.

PREGUNTA	SI	NO	OBSEVACION
• ¿Existe una descripción de los procesos que deben desempeñar los diferentes usuarios?			
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos de la red, servicios de red, etc.) que debe cumplir el personal encargado del funcionamiento del hardware?			
7. ¿Existe un manual de funciones para el personal encargado del funcionamiento del hardware de los equipos de cómputo?			
8. El manual de funciones para los usuarios que interactúan con el hardware de los equipos de computo, cumple con los siguientes requisitos: • ¿Existe una identificación clara de los diferentes cargos o roles que los funcionarios pueden desempeñar?			
• ¿Están claramente definidas las funciones (mantenimiento preventivo, correctivo, manejo de los equipos, servicios, etc.) que debe cumplir el personal encargado del funcionamiento del hardware?			
9. ¿Existen planes de contingencia para reemplazar a algunos funcionarios en caso de ausencia?			
10. El plan de contingencia para reemplazar a empleados cumple con los siguientes requisitos: • ¿Procedimientos para la contratación de personal de reemplazo?			
• ¿Está documentado?			
11. ¿Existen personas claves en la operación, administración y funcionamiento del hardware?			
12. ¿Existe personal indispensable que opere o administre el hardware?			
13. ¿Existen políticas y procedimientos para realizar la contratación de personal nuevo?			

¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN PO9_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.				**PAGINA**	
					1 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Servidores, Comunicaciones y Equipos de Cómputo.			
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez					
MATERIAL DE	COBIT					
	Planeación y Organización (PO)		**PROCESO**	Evaluación de riesgos de TI (PO9)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de los servidores?				
2. Estas políticas, procedimientos o metodologías contemplan: • ¿Los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?				
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los servidores?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los servidores?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de los servidores?				
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?				
• ¿La identificación de controles que mitiguen los riesgos?				
• ¿Toma de decisiones frente a los riesgos? (riesgos aceptables y cuales deben mitigarse).				
• ¿La elaboración del Plan de Seguridad Informática?(que acciones de deben llevar a cabo para mitigar los riesgos)				
• ¿La ejecución del Plan de Seguridad Informática?				
3. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de las comunicaciones?				
4. Estas políticas, procedimientos o metodologías contemplan:				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted!		PLAN PO9_2_SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	2 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Servidores, Comunicaciones y Equipos de Cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Evaluación de riesgos de TI (PO9)		

PREGUNTA	SI	NO	NA	FUENTE
• ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?				
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de las comunicaciones?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de las comunicaciones?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de las comunicaciones?				
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?				
• ¿La identificación de controles que mitiguen los riesgos?				
• ¿La toma de decisiones frente a los riesgos?(Cuales riesgos son aceptables y cuales riesgos deben mitigarse)				
• ¿La elaboración del Plan de Seguridad Informática?(que acciones de deben llevar a cabo para mitigar los riesgos)				
• ¿La ejecución del Plan de Seguridad Informática?				
5. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de los equipos de cómputo?				
6. Estas políticas, procedimientos o metodologías contemplan:				
• ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN PO9_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Servidores, Comunicaciones y Equipos de Cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Evaluación de riesgos de TI (PO9)		

PREGUNTA	SI	NO	NA	FUENTE
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los equipos de cómputo?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los equipos de cómputo?				
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de los equipos de cómputo?				
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?				
• ¿La identificación de controles que mitiguen los riesgos?				
• ¿La toma de decisiones frente a los riesgos?(Cuales riesgos son aceptables y cuales riesgos deben mitigarse)				
• ¿La elaboración del plan de seguridad informática?(que acciones de deben llevar a cabo para mitigar los riesgos)				
• ¿La ejecución del Plan de Seguridad Informática?				
7. ¿Existen políticas o procedimientos para la adquisición de pólizas de seguros para el manejo del riesgo?				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** ENT_PO9_SP

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA** 1 DE 3	
ÁREA AUDITAD	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores		

ENTREVISTADO	Ing. Diego Bastidas
CARGO	Auxiliar De Soporte Y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
1. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de los servidores?			
2. Estas políticas, procedimientos o metodologías			
• ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?			
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los servidores?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los servidores?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de los servidores?			
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?			
• ¿La identificación de controles que mitiguen los riesgos?			
• ¿La toma de decisiones frente a los riesgos?(Cuales riesgos son aceptables y cuales riesgos deben mitigarse)			
• ¿La elaboración del Plan de Seguridad Informática?(que acciones de deben llevar a cabo para mitigar los riesgos)			
• ¿La ejecución del Plan de Seguridad Informática?			
3. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de las comunicaciones?			
4. Estas políticas, procedimientos o metodologías contemplan:			
• ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?			
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de las comunicaciones?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de las comunicaciones?			

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** ENT_PO9_SP

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA** 2 DE 3	
ÁREA AUDITAD	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores		

ENTREVISTADO	Ing. Diego Bastidas
CARGO	Auxiliar De Soporte Y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
5. Estas políticas, procedimientos o metodologías contemplan: • ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?			
6. Estas políticas, procedimientos o metodologías contemplan: • ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?			
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de las comunicaciones?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de las comunicaciones?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de las comunicaciones?			
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?			
• ¿La identificación de controles que mitiguen los riesgos?			
• ¿La toma de decisiones frente a los riesgos?(Cuales riesgos son aceptables y cuales riesgos deben mitigarse)			
• ¿La elaboración del Plan de Seguridad Informática?(que acciones de deben llevar a cabo para mitigar los riesgos)			
• ¿La ejecución del Plan de Seguridad Informática?			
7. ¿En Emssanar ESS existen procedimientos o metodologías para el análisis y gestión de riesgos del hardware de los equipos de cómputo?			
8. Estas políticas, procedimientos o metodologías contemplan:			
• ¿El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos?			

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** ENT_PO9_SP

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA** 3 DE 3	
ÁREA AUDITAD	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores		

ENTREVISTADO	Ing. Diego Bastidas
CARGO	Auxiliar De Soporte Y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
• ¿La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los equipos de cómputo?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los equipos de cómputo?			
• ¿La determinación de la probabilidad de ocurrencia de los riesgos que amenazan la seguridad del hardware de los equipos de cómputo? •			
• ¿La determinación del impacto que causaría la ocurrencia de los riesgos?			
• ¿La identificación de controles que mitiguen los riesgos?			
• ¿La toma de decisiones frente a los riesgos?(Cuales riesgos son aceptables y cuales riesgos deben mitigarse)			
• ¿La elaboración del Plan de Seguridad Informática?(que acciones de deben llevar a cabo para mitigar los riesgos)			
• ¿La ejecución del Plan de Seguridad Informática?			
9. ¿Existen políticas o procedimientos para la adquisición de pólizas de seguros para el manejo del riesgo?			

¡Siempre cerca de Usted !	**ENTREVISTA**	**REF** ENT PO9_CC

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA**		
				1	DE	2
ÁREA AUDITADA	Sistemas	**SISTEMA**	Servidores			
OBJETIVO ENTREVISTA	Evaluar el hardware de los servidores, especificaciones técnicas y su mantenimiento					

ENTREVISTADO	Lucia Delgado
CARGO	Agente De Contactos – Centro De Contactos

1. ¿En qué consiste su cargo?

2. Describa brevemente el uso que le da al equipo

3. Describa brevemente como es el desempeño del equipo que está operando

4. ¿Considera que las características del hardware del equipo son suficientes para el desempeño de su trabajo?

5. ¿Qué hace en caso de que el equipo falle? ¿a quien acude?

6. ¿conoce el proceso de dotación de nuevos equipos de cómputo o adquisición de hardware? ¿ha hecho uso de él?

7. ¿conoce y hace usos del manual de soporte técnico?

8. ¿conoce el proceso de rotación de equipos? ¿en qué consiste?

¡Siempre cerca de Usted !	**ENTREVISTA**	**REF** ENT PO9_CC

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S.			**PAGINA**		
				2	DE	2
ÁREA AUDITADA	Sistemas	**SISTEMA**	Servidores			
OBJETIVO ENTREVISTA	Evaluar el hardware de los servidores, especificaciones técnicas y su mantenimiento					

ENTREVISTADO	Lucia Delgado
CARGO	Agente De Contactos – Centro De Contactos

9. ¿conoce el cronograma de mantenimiento de los equipos?

_____
_____

10. ¿Quiénes son los encargados de llevar a cabo el mantenimiento?

_____
_____

11. ¿Considera usted que el mantenimiento que se le hace a los equipos es oportuno?

_____
_____

Dominio: adquisición e implementación (AI)

- ✓ **AI3 Adquirir y mantener infraestructura tecnológica**

La información que se busca obtener con la aplicación del cuestionario está relacionada con datos del mantenimiento del hardware de comunicaciones, servidores y equipos de cómputo, solicitudes de nuevo hardware.

Entrevista: confirmar información suministrada en el cuestionario, también recolectar información en cuanto a políticas, administración y gestión de la red de comunicaciones. También se realiza entrevista con preguntas abiertas que servirá para recolectar información con respecto al funcionamiento y mantenimiento de la red de comunicaciones.

- ✓ **AI5 Adquirir recursos de TI**

Con la aplicación del cuestionario se busca obtener información concerniente al proceso de adquirir nuevo hardware.

Entrevista: recolectar información con respecto al manejo de proveedores, contratos, etc.

- ✓ **AI6 Administrar cambios**

Con la aplicación del cuestionario se busca obtener información concerniente al manejo de los cambios de la infraestructura tecnológica.

¡Siempre cerca de Usted !	**CUESTIONARIO**	**REF** **PLAN AI3_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	1 DE 5
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica (AI3)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existe personal capacitado para el manejo, adquisición y mantenimiento de la infraestructura Tecnológica?				
2. ¿Existe un procedimiento o políticas para la adquisición del hardware (comunicaciones y servidores)?				
3. Estas políticas o procedimientos contiene: • La solicitud de nuevas adquisiciones de hardware (equipos de comunicación) y sus				
• La solicitud de nuevas adquisiciones de hardware (servidores) y sus especificaciones.				
• El análisis y evaluación de las solicitudes.				
• La aprobación de la adquisición de hardware.				
• La recepción y análisis de cotizaciones a diferentes proveedores del hardware.				
• Elección de la mejor propuesta de los proveedores (calidad, costo y garantía) para la compra del hardware.				
4. ¿Los funcionarios del área de sistemas son conocedores de estas políticas?				
5. ¿Existe documentación de la información anterior?				
6. ¿Existe un plan de mantenimiento de la infraestructura tecnológica?				
7. El plan de mantenimiento de infraestructura tecnológica contiene: • Mantenimiento preventivo del hardware de comunicaciones.				
• Mantenimiento preventivo del hardware de servidores				
• Mantenimiento correctivo del hardware de comunicaciones.				

¡Siempre cerca de Usted !	**CUESTIONARIO**	**REF** **PLAN AI3_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 2 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica (AI3)		

PREGUNTA	SI	NO	NA	FUENTE
• Mantenimiento correctivo del hardware de servidores.				
8. En cuanto al mantenimiento preventivo del hardware se realiza • Revisión de la Instalación de los equipos de comunicaciones				
• Revisión de la Instalación de los servidores				
• La revisión periódica del estado de los equipos de comunicaciones.				
• La revisión periódica del estado de los equipos de los servidores.				
• Limpieza física (utilizando sopladoras, cremas, productos químicos especializados, etc.) de los equipos de computo				
• Limpieza física (utilizando sopladoras, cremas, productos químicos especializados, etc.) de los servidores.				
9. En cuanto al mantenimiento correctivo se realiza: • Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, board, tarjeta de red, tarjeta de video, etc.) que conforman un servidor.				
• Reemplazo del dispositivo defectuoso				
• Reparación del dispositivo defectuoso				
• Pruebas de funcionamiento de la terminal una vez realizados el mantenimiento.				
• Pruebas de funcionamiento de cada uno de los dispositivos de comunicación (Módems, Hubs, Repetidores, bridges, Routers, Gateways, etc)				
10. ¿Existe el manual de funciones para el personal encargado de realizar el mantenimiento preventivo y correctivo de los equipos de cómputo?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO**	**REF** **PLAN AI3_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 DE 5
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica (AI3)	

PREGUNTA	SI	NO	NA	FUENTE
11. ¿Existe el manual de funciones para el personal encargado de realizar el mantenimiento preventivo y correctivo de los equipos de comunicaciones?				
12. ¿Existe el manual de funciones para el personal encargado de realizar el mantenimiento preventivo y correctivo de los servidores?				
13. ¿El manual de funciones para el personal encargado de realizar estas funciones, tiene en cuenta: • ¿Descripción del cargo y perfil del funcionario encargado de realizar el mantenimiento preventivo y correctivo de los equipos de comunicaciones y servidores?				
• Descripción detallada de los procedimientos a seguir dependiendo del caso a revisar (daño de disco duro, daño de CPU, daño de monitor, etc.)				
14. ¿Dentro del personal de mantenimiento existe una persona preparada/especialista en reparaciones eléctricas (redes eléctricas, etc.)?				
15. ¿Dentro del personal de mantenimiento existe un especialista en reparación de equipos de comunicación?				
16. ¿Dentro del personal de mantenimiento existe un especialista en reparación de servidores?				
17. ¿Dentro del personal de mantenimiento existe un especialista en redes?				
18. ¿El personal encargado de realizar el procedimiento de mantenimiento preventivo y correctivo de los equipos de comunicación, tiene la capacidad y la experiencia para hacerlo?				
19. El personal encargado de realizar el procedimiento de mantenimiento preventivo y correctivo de los servidores, tiene la capacidad y la experiencia para hacerlo?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO**	**REF** **PLAN AI3_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	4 DE 5
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica (AI3)		

PREGUNTA	SI	NO	NA	FUENTE
20. ¿Existe en Emssanar un inventario detallado de los elementos de hardware que soportan el normal funcionamiento de la red de comunicaciones?				
21. ¿Existe en Emssanar un inventario detallado de los elementos de hardware que soportan el normal funcionamiento de los servidores?				
22. Periódicamente se lleva a cabo un control de la actualización del inventario: • Trimestral				
• Semestral				
• Anual				
23. Para los equipos de computo (servidor, terminales) este inventario tiene en cuenta: • Características del procesador (nombre de referencia, modelo, familia, velocidad, etc.)				
• Características de la memoria RAM (capacidad instalada, capacidad máxima, tipo de				
• Características de la placa madre (modelo, nombre del fabricante, etc.)				
• Características del disco duro (modelo, capacidad almacenamiento, etc.)				
• Características del disco duro (modelo, capacidad almacenamiento, etc.)				
• Características generales (modelo, referencia, marca, etc.) de periféricos (teclado, monitor, Mouse, etc.)				
• Licencia (en caso de necesitarse) del Sistema Operativo instalado				

	CUESTIONARIO	REF
¡Siempre cerca de Usted !		PLAN AI3_2_SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	5 DE 5
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica (AI3)		

PREGUNTA	SI	NO	NA	FUENTE
• Relación del hardware instalado				
24. ¿Cuando se presenta un daño o caída de la red en una terminal de trabajo o del servidor, existe un procedimiento a seguir?				
25. ¿Este procedimiento contempla: • Realización por parte del funcionario responsable del equipo, de una solicitud por escrito para la revisión del equipo.				
• Entrega (mediante acta o documento) por parte del funcionario del equipo dañado al personal de mantenimiento.				
• Recepción (mediante acta o documento) por parte de personal de mantenimiento del equipo a revisar.				
• Revisión y solución de acuerdo a las políticas y procedimientos estipulados para estos fines.				
• Entrega por parte del personal de mantenimiento y recepción por parte del funcionario que reporto el daño, del equipo de computo ya reparado.				
• El procedimiento de entrega y recepción de soluciones está documentada.				
26. ¿Este proceso es conocido por los funcionarios del área de sistemas?				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA** 1 DE 8	
ÁREA AUDITAD	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones,		

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
1. ¿ Existe personal encargado de administrar la Red?				
2. Quien opera y/o administra la Red es: • Ingeniero de sistemas				
• Técnico en sistemas				
• Tecnólogo en sistemas				
• Otro (cual)				
3. ¿ Existe un manual de funciones del manejo de Red (Servicios de red, mantenimiento, manejo de la red, soporte de hardware,				
4. ¿Existe diagrama de Red?				
5. La gestión de Red es manejada por: • Área de Sistemas				
• Contratación de un servicio tercerizado.				
6. Dentro de la gestión de red, se tiene en cuenta: • La planificación, organización, operación, mantenimiento y control de los elementos				
• Garantizar un nivel de servicio de acuerdo a				
• Permitir la capacidad de intercambio y procesamiento de información de gestión a fin de ayudar a la administración de la red a realizar sus actividades con eficiencia.				
7. ¿La gestión de red está documentada?				
8. El adecuado empleo de las tecnologías de gestión de red, permite: • Mejorar la eficiencia la disponibilidad y el desempeño de las redes.				
• Aumentar la relación calidad/costo en el diseño y operación de redes, ósea disminuir los costos de funcionamiento de una red y/o aumentar la calidad de servicio.				
• Aumentar la satisfacción de los usuarios.				
• Reducir la necesidad de recursos humanos en la operación de la red.				

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño		**PAGINA**	2 DE 8
ÁREA AUDITADA	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, servidores y equipos de cómputo.	

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
9. Para tener mayor eficiencia en la operación de la Red, se tiene en cuenta: • Recursos humanos (honestidad, creatividad, capacidad de respuesta rápida, motivación, relaciones humanas).				
• Desarrollo tecnológico (diseño de la red, operación, optimización, expansión, instalación y vida útil de la misma)				
• Métodos de trabajo (seguridad, configuración, fallos, etc).				
• Herramientas (plataforma de gestión)				
10. ¿El cumplimiento de los objetivos planificados para el área de comunicaciones se controla mediante: • Un servidor utilizado por el área de sistemas para monitorear las actividades de las distintas áreas.				
• Informes de avance periódicos elevados a las autoridades del área de sistemas.				
• Reportes de carácter informal.				
• Supervisión no documentada.				
11. El área de sistemas dispone de políticas, procedimientos y estándares documentados aprobados formalmente para las tareas: • Desarrollo y mantenimiento de la red.				
• Administración de la seguridad.				
• Tratamiento de contingencias.				
• Administración de copias de backups.				
• Otros				
12. ¿Cuántas líneas telefónicas hay en Emssanar?				
13. La incorporación de comunicaciones en el área de sistemas en Emssanar es realizada por:				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA** 3 DE 8	
ÁREA AUDITADA	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, servidores y equipos de cómputo.		

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Desarrollos realizados por un grupo externo.				
• Contratado y supervisado por el área de sistemas.				
• Desarrollos realizados por Ingenieros de sistemas, técnicos contratados por las áreas usuarias.				
• Provisión de sistemas o de equipos de comunicación por parte de otros organismos del Estado.				
• Otros (Cuales)				
14. La plataforma tecnológica del área de sistemas cuenta con: • Mainframe.				
• Servidores de tecnología Intel con sistemas operativos tipo Novell, Windows NT, Linux,				
• Servidores de tecnología RISC -S.O Unix.				
• Servidores de tecnología CISC con sistemas operativos Unix.				
• Servidores de tecnología CISC Y RISC (tecnología hibrida) de acuerdo al tipo				
• Otros servidores (AS/400, VAX, etc.).				
15. ¿En caso de caída de un servidor, se toman medidas de emergencia?				
16. Las medidas de emergencia tiene en cuenta: • Contar con servidores de respaldo.				
• Hardware disponible para dar soporte a fallos (memoria, disco duro, etc)				
• Actualización de tecnología para servidores.				
• Otros (cuales).				
17. ¿Cuántos servidores hay?				
18. Los Tipos de Servicios montados en servidores que maneja Emssanar son: rvidor)				

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			PAGINA		
				4	DE	8
ÁREA AUDITADA	Sistemas.	OBJETO DE ESTUDIO	Hardware de Comunicaciones, servidores y equipos de cómputo.			

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Servidor de correo				
• Servidor de Base de Datos				
• Servidor de archivos (almacena varios archivos y distribuye a otros clientes en red).				
• Servidor de impresiones (controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red)				
• Servidor de fax				
• Servidor de la telefonía				
• Servidor Proxy				
• Servidor del acceso remoto (RAS)				
• Servidor de reserva				
• Otros (cuales)				
19. ¿Los servidores se conectan a la red mediante una interfaz que puede ser una red verdadera o mediante conexión vía línea telefónica o digital?				
20. ¿Existe documentación del hardware de los servidores?				
21. ¿Existen Hojas de vida de los servidores?				
22. En cuanto a equipos de computo, Emssanar dispone de: • Hasta 50 computadoras personales (PC).				
• Entre 51 y 100 PCs				
• Entre 101 y 500 PCs				
• Entre 501 y 1000 PCs				
• Más de 1000 PCs				
23. En cuanto a servicios, Emssanar dispone de:				
• Base de datos				

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			PAGINA		
				5	DE	8
ÁREA AUDITADA	Sistemas.	OBJETO DE ESTUDIO	Hardware de Comunicaciones, servidores y equipos de cómputo.			

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Sitio Web				
• Correo electrónico				
• Firewall				
• Intranet				
24. El sitio Web de Emssanar es utilizado para: • Difusión de información y/o servicios de carácter público.				
• Recepción de información.				
• Emisión de documentación.				
• Otro (cual)				
26. ¿En cuanto a Comunicaciones, existe un inventario de equipos de telecomunicaciones?				
27. Tipo de Red: • Red de Área Local (LAN)				
• Red de Área metropolitana (MAN)				
28. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
29. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
30. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
31. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
32. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
33. En cuanto a servicios, Emssanar dispone de: • Telefonía				
• Base de datos				
34. En cuanto a servicios, Emssanar dispone de: • Telefonía				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA**	
				6 DE 8	
ÁREA AUDITADA	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, servidores y equipos de cómputo.		

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Base de datos				
• Red de Área Amplia (WAN)				
35. Componentes de la red: • Servidores.				
• Estaciones de trabajo.				
• Sistema de cableado.				
• Recursos y periféricos compartidos (dispositivos de almacenamiento ligado al servidor como impresoras, discos ópticos				
36. Topología de la Red: • Topología en Bus				
• Topología anillo				
• Topología estrella				
37. Dispositivos de la Red: • Swicthes				
• Módems				
• Hubs				
• Repetidores				
• Bridges				
• Routers				
• Gateways				
38. Las redes de acceso disponibles en Emssanar: • Telefonía fija				
• Banda ancha				
• Telefonía móvil				
• Redes de televisión				
• Canal dedicado				
• Modem				
• Redes privadas virtuales VPNs				
• MPLS				
39. Según el tipo de tecnología, Emssanar EPS posee: • Líneas convencionales RTB (telefónica bas)				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA** 7 DE 8	
ÁREA AUDITADA	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, servidores y equipos de cómputo.		

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Líneas digitales por ADSL (Línea de Abonado Digital Asimétrica)				
• Líneas RDSI (Red digital de serv. integrados)				
40. Quien monitorea la red es: • Personal capacitado de la empresa				
• Proveedor de la red				
41. ¿Existe documentación de lo anterior?				
42. ¿Existen políticas o procedimientos para el mantenimiento de los servicios de la Red?				
43. Las políticas o procedimientos contienen: • Intervalos de tiempo fuera de servicio				
• Uso adecuado de internet				
• Tener habilitado servicios que se necesiten.				
• Reglamento de uso de herramientas				
44. ¿Estas políticas o procedimientos están				
45. ¿Existe un manual de red de comunicaciones y servicios?				
46. ¿Se tiene seguros sobre todos los equipos de comunicaciones?				
47. ¿Se tiene seguros sobre todos los equipos de servidores y equipos de cómputo?				
48. ¿Con que empresa o compañía? (pólizas de				
49. ¿Existen normas para el manejo de las comunicaciones?				
50. En cuanto a las normas, existen: • Normas de control de calidad				
• Normas ISO. (Cual).				
51. ¿Existen políticas propias de la empresa para el manejo de las comunicaciones?				
52. ¿Estas Normas y políticas se aplican y se				
53. ¿Existen proveedores de red?				
54. En cuanto a proveedores de red, están: • Telmex				
• Telefónica				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_2**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño			**PAGINA**	
				8 DE 8	
ÁREA AUDITADA	Sistemas.	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, servidores y equipos de cómputo.		

ENTREVISTADO	Diego Bastidas
CARGO	Auxiliar De Soporte Técnico Y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Comcel				
• Movistar				
• Otro (cual).				
55. ¿Existen políticas en cuanto a contratación de proveedores de red?				
56. Estas políticas, contienen: • Términos cumplimiento o incumplimiento de contratación por parte y parte.				
• Soporte y mantenimiento.				
• Garantías				
• Otros (cuales)				
57. ¿Estas políticas están documentadas?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI3_SP_1**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS Nariño			**PAGINA** 1 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de		
OBJETIVO DE LA ENTREVISTA	Evaluar la forma de comunicación, el uso y mantenimiento de los equipos de comunicaciones, de las diferentes sedes interconectadas.				

ENTREVISTADO	Diego Bastidas
CARGO	Asistente Técnico de Soporte y Mantenimiento.

1. ¿Cuál es la función de la sede _____?

   _____

   _____

2. ¿Describa como son la red de comunicaciones con la principal Emssanar ESS?

   _____

   _____

3. ¿Quién provee la Red de internet?

   _____

   _____

4. ¿En esta sede hay alguna persona encargada del manejo y control de la red de comunicaciones?

   _____

   _____

5. ¿Quién maneja la Red?

   _____

   _____

6. ¿Quién tiene Acceso a la Red?

   _____

   _____

7. ¿Con que Frecuencia se cambian las claves?

   _____

   _____

8. ¿En caso de caída de la red que procedimiento se sigue?

   _____

   _____

	ENTREVISTA	REF
¡Siempre cerca de Usted!		ENT_AI3_SP_1

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS Nariño			**PAGINA**	
				2 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de		
OBJETIVO DE LA ENTREVISTA	Evaluar la forma de comunicación, el uso y mantenimiento de los equipos de comunicaciones, de las diferentes sedes interconectadas.				

ENTREVISTADO	Diego Bastidas
CARGO	Asistente Técnico de Soporte y Mantenimiento.

9. En caso de dañarse algo con respecto a la red de comunicaciones y en cuanto a hardware de comunicaciones, ¿qué procedimiento sigue?

_____

_____

10. ¿Reporta la falla o caída de la Red al proveedor?

_____

_____

11. ¿Recibe solución inmediata de soporte técnico por parte de los proveedores?

_____

_____

12. ¿Qué equipos conforman la red de comunicaciones?

_____

_____

13. ¿El Cableado de red se acoge a la normas?

_____

_____

14. ¿La red de datos se encuentra certificada?

_____

_____

15. ¿Se realiza mantenimiento de la red de comunicaciones, cada cuanto?

_____

_____

16. ¿Se lleva un registro de mantenimiento de estos, cual?

_____

_____

	ENTREVISTA	REF
¡Siempre cerca de Usted!		ENT_AI3_SP_1

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS Nariño		**PAGINA**		
			3	DE	3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones		
OBJETIVO DE LA ENTREVISTA	Evaluar la forma de comunicación, el uso y mantenimiento de los equipos de comunicaciones, de las diferentes sedes interconectadas.				

ENTREVISTADO	Diego Bastidas
CARGO	Asistente Técnico de Soporte y Mantenimiento.

17. ¿Quién o quiénes son los responsables de este mantenimiento?

_____

_____

18. ¿Cuántos equipos están interconectados a la red?

_____

_____

19. ¿Qué tipo de conexión a la red tiene, Canal dedicado, banda ancha, enlace u otro? ¿Cuál?_____

_____

20. ¿En cuanto a los cuartos de Comunicación hay uno por cada piso?

_____

_____

21. ¿Se hace Mantenimiento a los cuartos de comunicación? ¿Cómo se hace la limpieza a los cuartos de comunicación?_____

_____

22. ¿Todas las sedes se comunican con el cuarto de telecomunicaciones principal? ¿A través de fibra óptica?_____

_____

23. ¿Existe acceso limitado a los cuartos de Telecomunicaciones? ¿Quiénes tienen acceso?_____

_____

24. ¿Tiene alguna recomendación para mejorar la comunicación con esta sede?

_____

_____

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO**	**REF** **PLAN AI5_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 1 DE 2
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo.	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir Recursos de TI (AI5)	

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas o procedimientos estándares relacionados con la adquisición de nuevos recursos TI (hardware)?				
2. Las políticas o procedimientos contienen lo siguiente: • Políticas de adquisición de recursos de TI (Hardware de comunicaciones y servidores).				
• Políticas de selección de nuevos proveedores.				
• Estándares de adquisición de hardware (Comunicaciones y servidores).				
3. Existen un procedimiento general para la adquisición de hardware en cuanto a: • Documentación de nuevas adquisiciones				
• Estándares de la nueva infraestructura adquirida.				
• Normas de instalación física de la Red				
4. ¿Existe en la empresa un procedimiento establecido para modificar y concluir contratos para todos los proveedores?				
5. ¿Se evalúa los contratos con proveedores en cuanto a la adquisición de recursos de hardware de comunicaciones?				
6. ¿Se evalúa los contratos con proveedores en cuanto a la adquisición de recursos de hardware de los servidores?				
7. El proceso de selección de proveedores tiene en cuenta: • Listado de proveedores acreditados para hacer la adquisición				
• La selección de proveedores se ajusta a los requerimientos de Emssanar.				
• Impacto ambiental.				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO**	**REF** **PLAN AI5_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 2 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquirir Recursos de TI (AI5)		

PREGUNTA	**SI**	**NO**	**NA**	**FUENTE**
• Análisis y evaluación financiera.				
8. Revisión y evaluación de los Contratos de adquisición con proveedores en cuanto a: • Pruebas de la tecnología adquirida.				
• Por parte de los proveedores, ofrecen servicios de asesoría técnica y/o capacitación.				
• Tiempo de garantía de los equipos a adquirir.				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI5_SP_1**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño		**PAGINA** 1 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores (Proveedores)	

ENTREVISTADO	Harold Caicedo
CARGO	Jefe de Sistemas

PREGUNTA	**SI**	**NO**	**CUANTOS**	**OBSERVACION**
1. ¿Emssanar, cuenta con un listado de proveedores acreditados para la adquisición de hardware y software necesario?				
2. ¿El área de sistemas cuenta con un proveedor de servicios para la instalación eléctrica?				
3. ¿Se contrata el mantenimiento del mismo con terceros?				
4. ¿El mantenimiento de la instalación eléctrica la realizan personal de la misma área de sistemas?				
5. ¿Existen políticas o procedimientos para la adquisición de hardware de comunicaciones y/o de servidores?				
6. ¿Estas políticas o procedimientos, tienen en cuenta: • La realización de una solicitud de compra formal y por escrito del hardware.				
• La solicitud describe las características que debe cumplir el hardware.				
• La solicitud describe la necesidad de adquisición del hardware.				
• La realización de varias cotizaciones y a diferentes proveedores del hardware a comprar.				
• Análisis (ej. Cuadros comparativos) de las propuestas de los proveedores.				
• Se elige la propuesta de adquisición de hardware más favorable (en cuanto a calidad, garantía y precios) para la entidad.				
7. ¿Estas políticas están documentadas?				
8. ¿En cuanto a contratos con proveedores: • Se establecen contratos de compraventa de hardware y software.				
• Se establecen contratos de licencia y mantenimiento relativos al hardware y software provenientes de terceros.				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_AI5_SP_1**

ENTIDAD AUDITADA	Empresa solidaria de Salud Emssanar ESS– Nariño		**PAGINA** 2 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones y servidores (Proveedores)	

ENTREVISTADO	Harold Caicedo
CARGO	Jefe de Sistemas

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
• Se establecen contratos de mantenimiento de soporte de Red.				
9. ¿Se realiza revisión detallada y continua de contratos con los proveedores?				
10. ¿Existe documentación de los contratos con proveedores?				
11. ¿Existen en el departamento de Sistemas, un inventario detallado de los elementos de hardware y software que soportan el normal funcionamiento de las comunicaciones?				
12. ¿Para los equipos de computo (servidor, terminales) este inventario tiene en cuenta: • Características de la memoria RAM (capacidad instalada, capacidad máxima, tipo de memoria, etc.)				
• Características del procesador (nombre de referencia, modelo, familia, velocidad, etc.)				
• Características de la placa madre (modelo, nombre del fabricante, etc.)				
• Características del disco duro (modelo, capacidad almacenamiento, etc.)				
• Características generales (modelo, referencia, marca, etc.) de los periféricos (teclado, monitor, Mouse, etc.)				
• Licencia (en caso de necesitarse) del Sistema Operativo instalado.				
• Licencia (en caso de necesitarse) del software instalado.				
• Características del disco duro (modelo, capacidad almacenamiento, etc.)				
13. . ¿Existe documentación del inventario de Hardware?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN AI6_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 1 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administrar Cambios (AI6)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existe algún procedimiento definido para realizar cambios en la infraestructura tecnológica?				
2. ¿Los procedimientos para el control de cambios tiene en cuenta los siguientes puntos: • Solicitud formal de cambios				
• Análisis, estudio y aprobación o reprobación de la solicitud de cambios				
• Priorización de solicitudes de cambios				
3. ¿Existe un reporte de solicitudes de cambio?				
4. El reporte de las solicitudes tiene en cuenta: • Control de las solicitudes de cambios.				
• Seguimiento de los cambios.				
• Aprobación de los cambios.				
• Listado de prioridades de las solicitudes aceptadas				
• Solución de los cambios				
• Fijación de Fecha de solución a los cambios aprobados				
• Cumplimiento de los cambios previstos.				
5. ¿Existe un proceso de revisión para garantizar la implantación completa de los cambios?				
• Existe un responsable de cada cambio.				

¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN AI6_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 2 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administrar Cambios (AI6)		

PREGUNTA	**SI**	**NO**	**NA**	**FUENTE**
• Se lleva un registro de los cambios realizados.				
• Se realiza una evaluación de los cambios realizados.				
6. ¿El proceso de cambios en la infraestructura tecnológica está documentada?				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

Entrega de servicio y soporte (DS)

- ✓ **Garantizar la continuidad del servicio (DS4)**

Con la aplicación del cuestionario, se pretende recolectar información concerniente a la continuidad de los servicios que se ofrecen dentro del área de sistemas.

- ✓ **Administrar la mesa de servicios y los incidentes (DS8)**

Con la aplicación del cuestionario se busca obtener información concerniente al proceso de soporte y mantenimiento de equipos., cuestionario que se aplico a algunos directivos de las diferentes sedes.

Entrevista: a través de una entrevista con tipo de preguntas abiertas confirmar información suministrada en el cuestionario en cuanto a la prestación de servicio de soporte y mantenimiento.

- ✓ **Administración del ambiente físico (DS12)**

Con la Aplicación del cuestionario se busca recolectar información concerniente a la administración del ambiente físico, enfocado a la seguridad de los equipos de comunicación, servidores y equipos de cómputo, control de seguridad del personal que ingresa a las sedes, etc.

Entrevista: confirmar la información suministrada en los cuestionarios con respecto a la seguridad física de los equipos y la planta física de la empresa.

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS4-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Garantizar la continuidad del servicio (DS4)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas y estrategias para garantizar la continuidad de los servicios de TI para las comunicaciones en Emssanar EPS?				
2. ¿En el POA se encuentran contempladas las políticas de continuidad de los servicios TI?				
3. Las políticas de continuidad del los servicios, está conformado por: • Roles y responsabilidades del personal de aseguramiento de la continuidad de los servicios de TI				
• Políticas y lineamientos necesarios para guiar las acciones de prevención de desastres y para asegurar que se cuenta con los planes necesarios para enfrentar y recuperarse de un desastre, con el menor impacto posible				
• Definición del esquema de análisis de riesgo.				
• Reglas y políticas para documentar y distribuir los planes.				
• Definición de políticas para la aprobación de los correspondientes planes				
4. ¿Las políticas de continuidad de los servicios de TI, contemplan una estrategia de continuidad alineada con la estrategia de continuidad de la Empresa?				
5. ¿Las políticas de continuidad de los servicios de TI, contemplan la identificación de los procesos críticos y el análisis del impacto?				
6. ¿Las políticas de los servicios de TI, contemplan la existencia de un Plan de continuidad o				
7. El Plan de Continuidad o POA contiene: • ¿Guía de cómo utilizar el Plan?				

Emssanar E.S.S. ¡Siempre cerca de Usted !	**CUESTIONARIO CUANTITATIVO**	**REF** PLAN DS4-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 2 DE 2
ÁREA AUDITADA	Sistemas	**OBJETO DE**	Hardware de comunicaciones, servidores y equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Garantizar la continuidad del servicio (DS4)	

PREGUNTA	SI	NO	NA	FUENTE
• ¿Identificación de tiempo fuera de servicio del hardware de comunicaciones?				
• ¿Identificación de tiempo fuera de servicio de los servidores?				
• Identificación crítica de personas afectadas y de los responsables por cada función del Plan				
• Existe un plan de acción				
8. ¿Existe control, actualización y mantenimientos del plan de continuidad o Plan Operativo Anual				
9. ¿Existe una persona encargada del control y la actualización del plan de continuidad o POA?				
10. ¿Las políticas de continuidad de los servicios de TI, contemplan la identificación de estrategias de continuidad?				
11. ¿Las políticas de continuidad de los servicios de TI, contemplan la realización de pruebas y la actualización del Plan de Continuidad?				
12. En las pruebas realizadas se incluyen: • Verificación de la totalidad y precisión del Plan				
• Evaluación del desempeño del personal involucrado				
• Identificar la capacidad de recuperar registros e información importante?				
13. ¿Las estrategias y políticas de continuidad de los servicios de TI, están documentadas?				
14. ¿Las estrategias y políticas de continuidad de los servicios de TI, son conocidas por los				
TOTALES				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = %

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS8-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 1	
ÁREA AUDITADA		**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administrar la mesa de servicios y los incidentes (DS8)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas y procedimientos para dar solución a problemas de usuarios relacionados con servidores y comunicaciones?				
2. ¿Existe una mesa de ayuda técnica para resolver problemas técnicos de hardware (comunicaciones y servidores)?				
3. ¿Existen políticas y procedimientos para priorizar problemas de usuarios relacionados con servidores?				
4. ¿Existen políticas y procedimientos para priorizar problemas de usuarios relacionados con las comunicaciones?				
5. ¿Existe un manual de funciones de la mesa de servicios?				
6. ¿Está definido un intervalo de tiempo para atender llamadas?				
7. En cuanto al intervalo de tiempo, está definido como: • Tiempo de respuesta inmediata				
• Tiempo respuesta a largo plazo				
• Intervalo de tiempo de acuerdo a la complejidad del problema.				
8. ¿La función de la mesa de servicios es atender, registrar, comunicar y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información?				
9. ¿Se evalúa de forma permanente el funcionamiento de la mesa de servicio?				
10. ¿Se garantiza la calidad de los servicios de TI dentro de la mesa de servicios?				
11. ¿Se da solución oportuna en un determinado tiempo a los problemas e incidentes reportados a la mesa de servicios?				

Emssanar E.S.S. ¡Siempre cerca de Usted!	ENTREVISTA	REF ENT_DS8_SP_1

ENTIDAD AUDITADA	Empresa Solidaria de Salud Emssanar ESS			**PAGINA** 1 DE 2	
ÁREA AUDITADA	Sistemas	**SISTEMA**	Comunicaciones, servidores y equipos		
OBJETIVO ENTREVISTA	Evaluar de que manera la mesa de servicios presta atención y soluciona problemas de hardware (comunicaciones, servidores y				

ENTREVISTADO	Diego Bastidas
CARGO	Asistente de Soporte y Mantenimiento

1. ¿Qué estrategias se utilizan para garantizar la continuidad de las comunicaciones?
   _____
   _____

2. ¿Qué estrategias se utilizan para garantizar la continuidad de los servicios de los servidores?_____
   _____

3. ¿Qué procedimientos se siguen para dar solución a problemas de usuarios relacionados con las comunicaciones? _____
   _____

4. ¿Qué procedimientos se siguen para dar solución a problemas de usuarios relacionados con los servidores?_____
   _____

5. ¿Existe una mesa de servicios? _____
   _____

6. ¿Cuáles son las principales funciones de la mesa de servicios? _____
   _____

7. ¿De qué manera se atienden los problemas que se reportan a la mesa de servicios?
   _____
   _____

8. ¿Se le da prioridad a los problemas según el caso? _____
   _____

9. ¿Aproximadamente en cuanto tiempo es solucionado un problema reportado a la mesa de servicios?_____
   _____

10. ¿De qué manera califica la atención de la mesa de servicios?
    _____
    _____

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS8-2-E.IPS

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 1	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administrar la mesa de servicios y los incidentes (DS8)		

REGUNTA	SI	NO	NA	FUENTE
1. ¿Existe una mesa de servicios donde usted pueda reportar problemas técnicos de la red de comunicaciones o de los equipos de cómputo?				
2. ¿Considera usted que el tiempo que se tarda la mesa de ayuda en dar solución a los problemas técnicos es el adecuado?				
3. ¿Considera usted que la solución que se da a los problemas técnicos es eficiente?				
4. ¿Considera usted que se da prioridad a los problemas técnicos dependiendo del caso?				
5. El tiempo de atención a llamadas para reportar problemas técnicos es: • Tiempo de respuesta inmediata				
• Tiempo de respuesta a mediano plazo				
• Tiempo de respuesta a largo plazo.				
6. ¿La mesa de ayuda atiende, analiza y da solución oportuna a todos los incidentes reportados, requerimientos de servicio y solicitudes de información?				
7. El servicio y la atención de la mesa de ayuda es: • Bueno				
• Regular				
• Deficiente				
TOTALES				
TOTAL ENCUESTA				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORT	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
Acceso a las instalaciones				
1. ¿Existen políticas y procedimientos de seguridad para el acceso y salida de las instalaciones de Emssanar EPS en el área de sistemas?				
2. Dentro de las políticas de seguridad para controlar la entrada y salida a las instalaciones de Emssanar, se tiene en cuenta: • Que todos los individuos que entran a las instalaciones, se identifique, sean autenticados y autorizados.				
• Realización de requisas a las personas que ingresan y que salen de las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que salen de las instalaciones.				
• Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.				
• Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones.				
3. ¿Existen controles para restringir el acceso físico de las personas al área de sistemas?				
4. ¿Existen controles para restringir el acceso físico de otros (público en general) a el área de sistemas?				
5. ¿Las condiciones físicas donde se encuentran los equipos de cómputo cumplen con los requerimientos de seguridad establecidos?				
6. Las instalaciones del centro de computo, cumplen con los requerimientos en cuanto a: • Espacio y movilidad. Posibilidades de movilidad de los equipos, suelo fijo, posibilidad de las personas, etc.				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				2 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
Condiciones físicas				
• Características de las salas altura, anchura, posición de las columnas.				
• Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.				
• Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.				
• Equipos de aire acondicionado deben estar en zona segura.				
• Sistemas de ventilación. Las instalaciones del centro de cómputo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.				
• Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios				
• Los materiales del centro de computo son incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.).				
• Los materiales del centro de computo son incombustibles.				
• Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.				
• Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
7. ¿El lugar donde actualmente se encuentran instalados los equipos de computo claves (servidores, routers, switches, etc.) que soportan el funcionamiento de la red de comunicaciones, cumple con los requerimientos de: • Espacio y movilidad				
• Iluminación				
• Tratamiento acústico				
• Sistemas de ventilación				
• Seguridad física				
• Suministro eléctrico				
• Polo a tierra				
• Tablero eléctrico independiente				
8. ¿Existen controles y/o procedimientos para restringir el acceso físico a las instalaciones donde se encuentran ubicados los servidores y demás equipos claves que soportan el funcionamiento de estos?				
9. ¿Los controles y/o procedimientos para restringir el acceso, tienen en cuenta: • Permitir solamente el acceso al personal de Tecnologías de la Información autorizado.				
• Existen elementos físicos (puertas, cerraduras, etc.) para evitar y controlar el acceso no autorizado				
• Estos elementos físicos se encuentran en buen estado y funcionando				
10. ¿Existen pólizas de seguros para los elementos de Tecnologías de la Información?				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				4 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen extintores de incendios ubicados en sitios estratégicos y de fácil acceso dentro de las instalaciones del departamento de sistemas?				
2. ¿Existen dispositivos detectores de humo, detectores de calor y supresores de incendios dentro de las instalaciones del departamento de sistemas?				
Plan de Contingencia				
3. ¿Existen planes de contingencia?				
4. ¿Existen planes de evacuación de las instalaciones de Emssanar, en caso de presentarse una erupción volcánica?				
5. ¿Estos planes están documentados?				
6. ¿Estos planes son de conocimiento del personal que labora en las instalaciones del departamento de sistemas y de Emssanar?				
7. ¿Existen señales que indiquen la ruta de evacuación de las instalaciones del departamento de sistemas?				
8. ¿Existen planos de las instalaciones y la distribución de los equipos de cómputo?				
9. ¿Existen sistemas de alarma y detección de movimiento en las instalaciones del departamento de sistemas?				
10. ¿Los sistemas de alarma y detección de movimiento están actualmente funcionando?				
11. ¿Existen sistemas de UPS que soportan el funcionamiento del servidor en caso de presentarse alteraciones en el fluido eléctrico?				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				5 DE 5	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
11. ¿Los Sistemas de UPS, cuentan con medidas que garanticen su seguridad?				
12. ¿Existen plantas eléctricas, que garanticen la continuidad de los servicios?				
13. ¿En caso de no tener fluido eléctrico por un largo periodo, se toman medidas del caso?				
14. En cuanto a las medidas que se toman, esta: • Plantas eléctricas				
15. ¿Existen cámaras de seguridad y vigilancia en las instalaciones de Emssanar?				
16. ¿Existen planos de la infraestructura física y del cableado estructurado?				
17. ¿El cableado de la red de datos está integrado a la estructura del edificio?				
18. ¿El cableado que no está integrado a la estructura del edificio, cuenta con medidas de protección o aislamientos (canaletas)?				
19. ¿Las canaletas del cableado es de: • Metálico				
• Plástico				
• Empotrado				
20. ¿Existe documentación de todo lo anterior?				
TOTALES				
TOTAL ENCUESTA				

PORCENTAJE DE RIESGO: _____ **=** _____ = %

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT DS12 SP 1**

ENTIDAD AUDITADA	**EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.**			**PAGINA** 1 DE 4	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones y servidores		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar De Soporte Y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
Acceso a las instalaciones			
1. ¿Existen políticas y procedimientos de seguridad para el acceso y salida de las instalaciones de Emssanar EPS en el área de sistemas?			
2. Dentro de las políticas de seguridad para controlar la entrada y salida a las instalaciones de Emssanar, se tiene en cuenta: • Que todos los individuos que entran a las instalaciones, se identifique, sean autenticados y autorizados.			
• Realización de requisas a las personas que ingresan y que salen de las instalaciones.			
• Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.			
• Registro de los equipos de computo (portátiles, PC, etc.) que salen de las instalaciones.			
• Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.			
• Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones.			
3. ¿Existen controles para restringir el acceso físico de las personas al área de sistemas?			
4. ¿Existen controles para restringir el acceso físico de otros (público en general) a el área de sistemas?			
5. ¿Las condiciones físicas donde se encuentran los equipos de cómputo cumplen con los requerimientos de seguridad establecidos?			
6. Las instalaciones del centro de computo, cumplen con los requerimientos en cuanto a: • Espacio y movilidad. Posibilidades de movilidad de los equipos, suelo fijo, posibilidad de las personas, etc.			
• Características de las salas altura, anchura, posición de las columnas.			

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT DS12 SP 1**

ENTIDAD AUDITADA	**EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.**			**PAGINA** 2 DE 4	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones y servidores		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar de Soporte y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
• Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.			
• Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, deben estar en zonas donde tanto el ruido como la vibración se encuentren			
• Equipos de aire acondicionado deben estar en zona segura.			
• Sistemas de ventilación. Las instalaciones del centro de cómputo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.			
• Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios			
• Los materiales del centro de computo son incombustibles (pintura de las paredes, suelo, techo, mesas,			
• Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.			
• Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de			
7. ¿El lugar donde actualmente se encuentran instalados los equipos de computo claves (servidores, routers, switches, etc.) que soportan el funcionamiento de la red de comunicaciones, cumple con los requerimientos de: • Espacio y movilidad			
• Iluminación			
• Tratamiento acústico			
• Sistemas de ventilación			

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT DS12 SP 1**

ENTIDAD AUDITADA	**EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.**			**PAGINA** 3 DE 4	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones y servidores		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar de Soporte y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
• Seguridad física			
• Suministro eléctrico			
• Polo a tierra			
• Tablero eléctrico independiente			
8. ¿Existen controles y/o procedimientos para restringir el acceso físico a las instalaciones donde se encuentran ubicados los servidores y demás equipos claves que soportan el funcionamiento de estos?			
9. ¿Los controles y/o procedimientos para restringir el acceso, tienen en cuenta: • Permitir solamente el acceso al personal de Tecnologías de la Información autorizado.			
• Existen elementos físicos (puertas, cerraduras, etc.) para evitar y controlar el acceso no autorizado.			
• Estos elementos físicos se encuentran en buen estado y funcionando			
10. ¿Existen pólizas de seguros para los elementos de Tecnologías de la Información?			
11. ¿Existen extintores de incendios ubicados en sitios estratégicos y de fácil acceso dentro de las instalaciones del departamento de sistemas?			
12. ¿Existen dispositivos detectores de humo, detectores de calor y supresores de incendios dentro de las instalaciones del departamento de sistemas?			
Plan de Contingencia			
13. ¿Existen planes de contingencia?			
14. ¿Existen planes de evacuación de las instalaciones de Emssanar, en caso de presentarse una erupción volcánica?			
15. ¿Estos planes están documentados?			
16. ¿Estos planes son de conocimiento del personal que labora en las instalaciones del departamento de sistemas y de Emssanar?			
17. ¿Existen señales que indiquen la ruta de evacuación de las instalaciones del departamento de sistemas?			

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT DS12 SP 1**

ENTIDAD AUDITADA	**EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.**			**PAGINA** 4 DE 4	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones y servidores		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar de Soporte y Mantenimiento

PREGUNTA	SI	NO	OBSERVACION
18. ¿Existen planos de las instalaciones y la distribución de los equipos de cómputo?			
19. ¿Existen sistemas de alarma y detección de movimiento en las instalaciones del departamento de sistemas?			
20. ¿Los sistemas de alarma y detección de movimiento están actualmente funcionando?			
21. ¿Existen sistemas de UPS que soportan el funcionamiento del servidor en caso de presentarse alteraciones en el fluido eléctrico?			
22. ¿Los Sistemas de UPS, cuentan con medidas que garanticen su seguridad?			
23. ¿Existen plantas eléctricas, que garanticen la continuidad de los servicios?			
24. ¿En caso de no tener fluido eléctrico por un largo periodo, se toman medidas del caso?			
25. En cuanto a las medidas que se toman, esta: • Plantas eléctricas			
• Otras			
26. ¿Existen cámaras de seguridad y vigilancia en las			
27. ¿Existen planos de la infraestructura física y del cableado			
28. ¿El cableado de la red de datos está integrado a la			
29. ¿El cableado que no está integrado a la estructura del edificio, cuenta con medidas de protección o aislamientos (canaletas)?			
30. ¿Las canaletas del cableado es de: • Metálico			
• Plástico			
• Empotrado			
31. ¿Existe documentación de todo lo anterior?			

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-E.IPS

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	SI	NO	NA	FUENTE
Acceso a las instalaciones				
1. ¿Existen medidas de seguridad para entrar y salir de las instalaciones de esta sede?				
2. En cuanto a las medidas de seguridad para controlar la entrada y salida de las instalaciones de la sede, se tiene en cuenta: • Que todos los individuos que entran a las instalaciones, se identifique, sean autenticados y autorizados				
• Realización de requisas a las personas que ingresan y que salen de las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que salen de las instalaciones.				
• La identificación, autenticación y autorización para el ingreso de visitantes que ingresan por el parqueadero. (vehículos y motocicletas).				
3. ¿Las condiciones físicas donde se encuentran los equipos de cómputo cumplen con los requerimientos de seguridad establecidos?				
4. Las instalaciones del centro de computo, cumplen con los requerimientos en cuanto a: • Espacio y movilidad. Posibilidades de movilidad de los equipos, suelo fijo, posibilidad de las				
• Características de las salas altura, anchura, posición de las columnas				
• El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.				
• Tratamiento acústico. (Los equipos ruidosos como las impresoras con impacto)				

¡Siempre cerca de Usted !	**CUESTIONARIO CUANTITATIVO**	**REF** PLAN DS12-2-E.IPS

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)		

PREGUNTA	**SI**	**NO**	**NA**	**FUENTE**
Acceso a las instalaciones				
5. ¿Existen medidas de seguridad para entrar y salir de las instalaciones de esta sede?				
6. En cuanto a las medidas de seguridad para controlar la entrada y salida de las instalaciones de la sede, se tiene en cuenta: • Que todos los individuos que entran a las instalaciones, se identifique, sean autenticados y autorizados				
• Realización de requisas a las personas que ingresan y que salen de las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.				
• Registro de los equipos de computo (portátiles, PC, etc.) que salen de las instalaciones.				
• La identificación, autenticación y autorización para el ingreso de visitantes que ingresan por el parqueadero. (vehículos y motocicletas).				
7. ¿Las condiciones físicas donde se encuentran los equipos de cómputo cumplen con los requerimientos de seguridad establecidos?				
8. Las instalaciones del centro de computo, cumplen con los requerimientos en cuanto a: • Espacio y movilidad. Posibilidades de movilidad de los equipos, suelo fijo, posibilidad de las personas.				
• Características de las salas altura, anchura, posición de las columnas				
• El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.				
• Tratamiento acústico. (Los equipos ruidosos como las impresoras con impacto)				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-E.IPS

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.		**PAGINA** 2 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)	

PREGUNTA	SI	NO	NA	FUENTE
Condiciones físicas				
• Equipos de aire acondicionado.				
• Sistemas de ventilación. Las instalaciones del centro de cómputo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por				
• Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios				
• Los materiales de las instalaciones donde se encuentran los equipos de computo son incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.).				
• Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.				
• El suministro eléctrico de las instalaciones y en particular la alimentación de los equipos, cuenta con condiciones especiales, como la utilización de una línea independiente del resto de la instalación con el fin de evitar interferencias.				
9. Dentro de las medidas de seguridad se tiene en cuenta: • Permitir solamente el acceso a personal autorizado				
• Existen elementos físicos (puertas, cerraduras, etc) para evitar y controlar el acceso no autorizado.				
• Estos elementos físicos se encuentran en buen estado y funcionando.				
10. ¿Existen extintores de incendio ubicados en sitios estratégicos y de fácil acceso dentro de las instalaciones del departamento o área de sistemas?				
11. ¿Existen dispositivos detectores de humo, detectores de calor y supresores de incendios dentro de las instalaciones del departamento de sistemas?				

	CUESTIONARIO CUANTITATIVO	REF
¡Siempre cerca de Usted !		PLAN DS12-2-E.IPS

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA** 3 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de servicios y soporte (DS)	**PROCESO**	Administración del Ambiente Físico (DS12)	

PREGUNTA	SI	NO	NA	FUENTE
12. ¿Se han realizado simulacros de evacuación de las instalaciones de la sede, en caso de presentarse una erupción volcánica?				
13. ¿Existen señales que indiquen la ruta de evacuación de las instalaciones de la sede?				
14. ¿Existen sistemas de alarma y detección de movimiento en las instalaciones de la sede?				
15. ¿Los sistemas de alarma y detección de movimiento están actualmente funcionando?				
16. ¿Existen sistemas de UPS que soportan el funcionamiento del los equipos de computo en caso de presentarse alteraciones en el fluido eléctrico?				
17. ¿Existen plantas eléctricas, que garanticen la continuidad de los servicios?				
18. ¿Existen cámaras de seguridad y vigilancia en las instalaciones de esta sede?				
TOTALES				
TOTAL ENCUESTA				

PORCENTAJE DE RIESGO: _____ **=** _____ = %

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_DS12_E.IPS_1**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones (Red Eléctrica)		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar de Soporte y Mantenimiento

PREGUNTA	SI	NO	CUANTOS	OBSERVACION
1. ¿La instalación eléctrica distribuye la energía eléctrica a los equipos conectados de una manera segura y eficiente?				
2. ¿La instalación eléctrica es flexible, es decir es susceptible de ampliarse, disminuirse o modificarse con facilidad, y según posibles				
3. ¿La instalación eléctrica es Segura, o sea garantiza la seguridad de las personas y propiedades durante su operación común?				
4. ¿Existe personal encargado del mantenimiento de la Red Eléctrica?				
5. ¿La instalación y suministro de energía es la				
6. ¿La instalación y suministro de energía cuenta con polo a tierra?				
7. ¿El polo a tierra cumple con las disposiciones del proveedor de equipos de cómputo?				
8. ¿El cableado se encuentra debidamente				
9. ¿Los cables de encuentran debidamente identificados (positivo, negativo, polo a tierra)?				
10. ¿Los contactos de equipo de cómputo están debidamente identificados?				
11. ¿En los contactos, está identificado el positivo, negativo y polo a tierra?				
12. ¿Se cuenta con los planos de instalación eléctrica actualizados?				
13. ¿Se tiene conectado a los contactos de equipos de cómputo otro equipo eléctrico?				
14. ¿Se tiene instalación eléctrica de equipos de cómputo independiente de otras instalaciones				
15. ¿Se tiene reguladores para los equipos de				
16. ¿Se verifica la regulación de las cargas máximas y mínimas?				
• En caso positivo, ¿Con que periodicidad?				

¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_DS12_E.IPS_1**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S.			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones (Red Eléctrica)		

ENTREVISTADO	Diego Ceballos
CARGO	Auxiliar de Soporte y Mantenimiento

	SI	NO	CUANTOS	OBSERVACION
17. ¿Se tiene equipo ininterrumpible (UPS)?				
• En caso positivo, ¿Dura el tiempo suficiente para respaldar los archivos o para continuar el proceso?				
• ¿Se Prueba su funcionamiento?				
18. ¿En caso de presentarse perdida de energía por un periodo prolongado, se tiene generadores de corriente ininterrumpida?				
19. En caso positivo, que tipo: • Plantas de luz de emergencia?				
• Otras, cuáles?				
19. ¿Se tiene Switche de apagado en caso de emergencia en lugar visible?				
20. ¿Los cables están dentro de paneles y canales eléctricos?				
21. ¿Existen tableros de distribución eléctrica?				
22. ¿Se evalúa continuamente la instalación				
23. ¿Existe documentación de la evaluación realizada?				

Dominio: monitorear y evaluar (ME)

- ✓ **Monitoreo y evaluación de desempeño de TI (ME1)**

Cuestionario aplicado con el fin de recolectar información concerniente al funcionamiento de los indicadores de funcionamiento del área de sistemas.

Entrevista: a través de una entrevista con tipo de preguntas abiertas confirmar la información suministrada en el cuestionario.

- ✓ **Monitoreo y evaluación de control interno (ME2)**

Cuestionario aplicado con el fin de recolectar información concerniente al manejo de los procesos de monitoreo de las actividades encaminadas a brindar seguridad física de los recursos TI.

¡Siempre cerca de Usted !	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN ME1_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			**PAGINA** 1 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo e Indicadores de funcionamiento.	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y Evaluar Desempeño de TI (ME1)	

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen indicadores de funcionamiento en el área de sistemas de Emssanar EPS?				
2. Existe un documento de los indicadores en los niveles de: • Cobertura				
• Obsolescencia				
• Soporte tecnológico				
• Tiempo fuera de servicio				
3. ¿Existen políticas que defina el cumplimiento de los indicadores?				
4. Existe una metodología de evaluación de los indicadores en cuanto a: • Al funcionamiento del nivel de cobertura.				
• Al funcionamiento del nivel de Soporte Tecnológico.				
• Al funcionamiento del nivel de tiempo fuera de servicio.				
• Al funcionamiento del nivel de Obsolescencia.				
5. Existe un método de control de monitoreo, de seguimiento en cuanto a la evaluación de los indicadores de funcionamiento respecto a: • Evolución histórica de los indicadores				
• El enfoque de los indicadores				
• El alcance de los indicadores				
• La metodología de los indicadores				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN ME1_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			**PAGINA** 2 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo e Indicadores de funcionamiento.	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y Evaluar Desempeño de TI (ME1)	

PREGUNTA	SI	NO	NA	FUENTE
• El Proceso de los indicadores				
• Medición de los indicadores				
6. ¿Hay balance de objetivos de desempeño de los indicadores con los de la empresa como tal?				
7. La evaluación del desempeño de los indicadores se realiza de forma: • Bimestral				
• Trimestral				
• Semestral				
• Anual				
8. ¿Existe un reporte de desempeño al consejo de dirección?				
9. ¿Se toman medidas correctivas en caso del incumplimiento de los indicadores?				
10. ¿Se asignan responsabilidades para la corrección?				
11. ¿Se rastrea los resultados de las acciones comprometidas?				
12. ¿Existe documentación de este proceso?				
13. ¿En cuanto al nivel de cobertura, hasta el presente año se ha cumplido con los objetivos?				
14. En cuanto al nivel de obsolescencia: • Se certifica la destrucción o baja de los equipos defectuosos				
• Se lleva un registro de los elementos (equipos de cómputo) dados de baja.				
• Se verifica la dada de baja de los equipos.				

Emssanar E.S.S. ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN ME1_2_SP**

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			**PAGINA** 3 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones, Servidores y Equipos de Computo e Indicadores de funcionamiento.	
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y Evaluar Desempeño de TI (ME1)	

PREGUNTA	**SI**	**NO**	**NA**	**FUENTE**
• Se tiene un responsable de este proceso				
TOTAL				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_ME1_SP_1**

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S			**PAGINA** 1 DE 3
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Indicadores de funcionamiento	
OBJETIVO DE LA ENTREVISTA	Evaluar el desempeño de TI en cuanto a los indicadores de funcionamiento en los diferentes niveles existentes en Emssanar, verificar el cumplimiento con los objetivos de cada uno.			

ENTREVISTADO	Harold Caicedo
CARGO	Jefe de Sistemas

1. ¿Existen indicadores de funcionamiento en el área de sistemas de Emssanar EPS?

2. ¿Cuál es el objetivo de la existencia de los indicadores?

3. ¿Cuántos indicadores y cuales existen en el área de sistemas de Emssanar E.P.S?

4. ¿Quién es el encargado de crear y diseñar metas para los indicadores?

5. ¿Cuáles son sus funciones dentro del manejo y control de los indicadores?

6. ¿Cada cuanto se analizan las metas de los indicadores?

7. ¿En qué consiste el indicador _____?

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_ME1_SP_1**

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S			**PAGINA** 2 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Indicadores de funcionamiento		
OBJETIVO DE LA ENTREVISTA	Evaluar el desempeño de TI en cuanto a los indicadores de funcionamiento en los diferentes niveles existentes en Emssanar, verificar el cumplimiento con los objetivos de cada uno.				

ENTREVISTADO	Harold Caicedo
CARGO	Jefe de Sistemas

8. ¿En qué consiste el indicador _____?

_____

_____

9. ¿En qué consiste el indicador _____?

_____

_____

10. ¿En qué consiste el indicador _____?

_____

_____

11. ¿Se evalúa continuamente el cumplimiento de estos?

_____

_____

12. ¿Cómo se evalúan los indicadores, y como se verifica que sean efectivos?

_____

_____

13. ¿Cuáles son los principales motivos para el incumplimiento de las metas de los indicadores?

_____

_____

Emssanar E.S.S. ¡Siempre cerca de Usted!	**ENTREVISTA**	**REF** **ENT_ME1_SP_1**

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S		**PAGINA** 3 DE 3	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Indicadores de funcionamiento	
OBJETIVO DE LA ENTREVISTA	Evaluar el desempeño de TI en cuanto a los indicadores de funcionamiento en los diferentes niveles existentes en Emssanar, verificar el cumplimiento con los objetivos de cada uno.			

ENTREVISTADO	Harold Caicedo
CARGO	Jefe de Sistemas

14. ¿Qué medidas se toman en caso del incumplimiento o encontrar anomalías en la evaluación?

_____

_____

15. ¿Existe un reporte de desempeño que se haga al consejo o al jefe de sistemas y en qué consiste?

_____

_____

16. ¿Existe documentación que soporte el cumplimiento de los indicadores?

_____

_____

	CUESTIONARIO	REF
¡Siempre cerca de Usted !		PLAN ME2_2_SP

ENTIDAD AUDITADA	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			**PAGINA**	
				1 DE 1	
ÁREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones de servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Quenguan y Edy Yanira Sánchez Perenguez				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Monitorear y Evaluar el Control Interno (ME2)		

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas o procedimiento relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física de los recursos Tecnológicos como hardware de servidores?				
2. ¿Existen políticas o procedimiento relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física de los recursos Tecnológicos como hardware de comunicaciones?				
3. ¿Existen políticas o procedimiento relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física de los recursos Tecnológicos como hardware de los equipos de computo?				
4. Se monitorea de forma continua, compara y mejora el ambiente de control de TI, en cuanto a: • Infraestructura de red.				
• Los servidores				
• Los equipos de Cómputo.				
4. ¿Se define quien va a realizar el monitoreo?				
5. ¿Se toman acciones correctivas de acuerdo al resultado de la evaluación del monitoreo de las actividades de TI?				
6. ¿Existe documentación de este proceso?				

PORCENTAJE DE RIESGO: _____ **=** _____ = = %

2.3.7 Hallazgos

Después de obtener los resultados de las diferentes técnicas aplicadas, se definen los riesgos encontrados, después de un análisis de acuerdo a cada caso de estudio.

Dominio: planeación y organización (PO)

De este dominio PO planeación y organización se seleccionaron los procesos PO3 Determinar la Dirección Tecnológica, PO4 Definición de la organización y las relaciones de TI, PO9 Evaluación de riesgos para ser evaluados, donde se identifican los riesgos encontrados.

- ✓ **PO3 Determinar la dirección tecnológica:** Los hallazgos o no conformidades encontradas se muestran así:

Emssanar E.S.S. ¡Siempre cerca de Usted!	**HALLAZGOS**	**REF** PLAN PO3_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S - Nariño			**PAGINA**	**1 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y organización (PO3)	**PROCESO**	Determinar la dirección tecnológica (PO3)		

HALLAZGO	**En Emssanar ESS,** el plan de contingencia en caso de que el hardware no funcione no está documentado. (SP)

RECOMENDACIONES

- En la empresa debe existir un documento de plan de contingencia que permita dar solución inmediata en caso de presentarse algún fallo en el hardware.
- El documento del plan de contingencia debe contener:
  - Objetivos claros para restaurar los servicio de forma rápida, eficiente y con el menor costo y pérdidas posibles.
  - Pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del los servicios.
  - Estrategias para la recuperación de desastres.
  - En cuanto a los diferentes niveles de daños, también se hace necesario presuponer el daño total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

IMPACTO	• El impacto que ocasiona un riesgo de este tipo es la dificultad de recuperación para seguir trabajando en un plazo mínimo después de que se haya presentado un problema, como por ejemplo la posibilidad de volver a la situación anterior, habiendo reemplazado y recuperado el máximo posible de los recursos e información. • En caso de presentarse un fallo del hardware bien sea de un equipo de computo o un servidor o un equipo de comunicaciones así haya un proceso practico a seguir este sería solo aplicable por un corto periodo, ya que en caso de un desastre la interrupción prolongada de los servicios de computación y comunicación pueden llevar a pérdidas financieras significativas y pérdida de credibilidad de los usuarios.

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S. ¡Siempre cerca de Usted!	**HALLAZGOS**	**REF** PLAN PO3_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S - Nariño			**PAGINA**	**2 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y organización (PO3)	**PROCESO**	Determinar la dirección tecnológica (PO3)		

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Bajo

EVIDENCIAS	ANEXO 32_ENT PO3_SP

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

- ✓ **PO4 Definir los procesos, organización y relaciones de TI:** en este proceso no se encontraron hallazgos.

- ✓ **PO9 Evaluación de riesgos:** Los hallazgos o no conformidades encontradas se muestran en así:

¡Siempre cerca de Usted !	**HALLAZGOS**	**REF** PLAN PO9_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S - **Nariño**				**PAGINA**	**1** **DE** **3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Riesgos del hardware de comunicaciones, servidores y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)			

HALLAZGO	En Emssanar ESS no hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones. (SP)

RECOMENDACIONES

- En Emssanar ESS debe existir un procedimiento que permita realizar el análisis y la gestión de riesgos para el funcionamiento del hardware de las comunicaciones, los equipos de computo y los servidores estos procedimientos deben contener:

  - Objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos.
  - La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los equipos de cómputo, los servidores y las comunicaciones.
  - La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones.
  - La determinación del impacto que causaría la ocurrencia de los riesgos.
  - La identificación de controles que mitiguen los riesgos.
  - La toma de decisiones frente a los riesgos.
  - La elaboración del Plan de Seguridad Informática que permita resguardar y mantener los recursos de TI.
  - La ejecución del Plan de Seguridad Informática.

- Es fundamental tener un método para realizar la gestión de riesgos que se integre dentro de la gestión de diferentes proyectos y que así mismo el equipo del proyecto esté involucrado en la identificación y seguimiento de los riesgos.

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S - **Nariño**				**PAGINA**		
					2	**DE**	**3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Riesgos del hardware de comunicaciones, servidores y equipos de cómputo.				
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P						
MATERIAL DE SOPORTE	COBIT						
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)				

Emssanar E.S.S.
¡Siempre cerca de Usted !

HALLAZGOS	**REF**
	PLAN PO9_3_1

RECOMENDACIONES
• Es importante que Emssanar ESS cuente con una herramienta que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del control informático.

IMPACTO	• La gestión de riesgo permite anticiparse al futuro y prevenir a la empresa de diferentes problemas en este caso riesgos que pongan en peligro el buen funcionamiento de Emssanar, y el no tener definido políticas de gestión de riesgos implica la toma de decisiones inmediata frente a un problema presentado sin tener previo análisis del riesgo ni tener la certeza de poder mitigar ese riesgo. • El que no exista personal encargado de la gestión de riesgos del hardware impide la identificación de los posibles riesgos y dado el caso llegase a presentar generaría lo siguiente: - Alto costo de la Gestión por Crisis - La presencia alta de sorpresas y problemas - Perder Ventaja Competitiva - Subir variaciones generales del proyecto - Disminuir la probabilidad de éxito del proyecto - Disminución de rentabilidad - Aumentar la probabilidad de la ocurrencia de que se presenten problemas.

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S - **Nariño**			**PAGINA**		
				2	**DE**	**3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Riesgos del hardware de comunicaciones, servidores y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)			

Emssanar E.S.S.
¡Siempre cerca de Usted !

HALLAZGOS

REF
PLAN PO9_3_1

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

EVIDENCIAS	ANEXO 14 PLAN PO9_2_SP

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

¡Siempre cerca de Usted !

HALLAZGOS

REF

PLAN_PO9_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				1	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Riesgos del hardware de comunicaciones, servidores y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)			

HALLAZGO	En la fundación Emssanar y en la IPS Lorenzo existen problemas de conectividad, baja velocidad, bloqueo y limitación de accesos a internet. (FE, LZ)

RECOMENDACIONES

- En Las sedes Fundación Emssanar y en la IPS Lorenzo continuamente se debe revisar el cronograma de mantenimiento o funcionamiento de la red, sobre todo en estas sedes, ya que el uso de internet es necesario para la implementación de diferentes proyectos y actividades que se desarrollan y así mismo no afectar el buen funcionamiento de estas.
- Se debe dar acceso a internet bajo restricciones que no afecte por completo los servicios que estas sedes necesitan utilizar para cumplir con sus funciones como tal.
- Se debe hacer un estudio más detallado de las sedes para priorizar que módulos o que funcionarios deben tener acceso a trabajar con mayor ancho de banda de a cuerdo a la función que desempeñen.

IMPACTO	• La falta de mantenimiento o revisión constante del funcionamiento de la red de internet, hace que se presente lentitud en los diferentes procesos que se trabaja en estas sedes. • La limitación de algunos servicios necesarios de internet hace que se presente indisposición por parte del personal para realizar algunas tareas de los diferentes proyectos que se adelantan dentro de estas sedes.

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

¡Siempre cerca de Usted !	**HALLAZGOS**	**REF** PLAN_PO9_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)		

PROBABILIDAD – IMPACTO			
Probabilidad	Medio	**Impacto**	Medio

EVIDENCIAS	ANEXO 34_ENT PO9_FE ANEXO 36_ENT PO9_LZ

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño		**RESPONSABLES**	**PAGINA**	
			EDY YANIRA SANCHEZ P.	**1**	**DE** **2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	LAURA YANETH NOGUERA Q.	Equipos de Computo.	
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)		

¡Siempre cerca de Usted !

HALLAZGOS	**REF**
	PLAN PO9_3_3

HALLAZGO	En las sedes Fundación Emssanar y en Cresemillas en la dependencia de Centro de Contactos existe deficiencia en cuanto al mantenimiento físico de los equipos y actualizaciones de programas de Antivirus. (FE, CC).

RECOMENDACIONES

- Concientización al personal que maneja los equipos de cómputo en cuanto al cuidado y limpieza de estos, puesto que también es responsabilidad de los mismos en el manejo de su herramienta de trabajo.
- Actualizar permanentemente el Programa de Antivirus.
- El personal de Soporte Técnico y Mantenimiento deberá mantener informado al jefe de esta dependencia igual con las demás sobre las fechas de mantenimiento, variaciones de los componentes y/o reubicaciones efectuadas a los equipos de computo, con el fin de mantenerlos actualizados.
- El desarrollo del mantenimiento se efectuara en conformidad con un cronograma establecido, el mismo será coordinado con los funcionarios a fin de tener toda la disponibilidad de los equipos sin afectar sus labores cotidianas.
- En la dependencia Centro de contactos de la sede Cresemillas la mayoría de los equipos permanecen encendidos las 24 horas para prestar el servicio de atención al cliente, razón justa para evaluar el cronograma de mantenimiento y reorganizarlo de tal forma que el mantenimiento preventivo sea más frecuente, muy importante visitar las sedes periódicamente que permita hacer una evaluación del comportamiento de todo lo que tiene que ver con el funcionamiento del hardware y actualizaciones de software que respondan a las necesidades de los usuarios que los operan y de igual forma responda al desempeño de su trabajo.

AUDITORES RESPONSABLES			
		EDY YANIRA SANCHEZ P.	PAGINA
		LAURA YANETH NOGUERA Q.	2 DE 2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño		
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Equipos de Computo.
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Planeación y organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)

¡Siempre cerca de Usted !

HALLAZGOS	**REF**
	PLAN PO9_3_3

IMPACTO	• La falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando en esta sede que los agentes de Contactos permanentemente tengan que estar cambiando de equipos que funcionen entre ellos generando incomodidad y retrasos en la atención a los usuarios y más aun cuando un equipo deja de funcionar generara más gastos ya que tendría que cambiarse o reemplazarse algunas piezas del hardware o en su defecto remplazo total de este, esto también provoca la disminución de vida útil de los equipos. • La desactualización de vacuna por tener internet con muy baja velocidad genera lentitud y pérdida de información, perjudicando las diferentes tareas de cada agente de contactos.

PROBABILIDAD – IMPACTO			
Probabilidad	Medio	**Impacto**	Medio

EVIDENCIAS	ANEXO 34_ENT PO9_FE ANEXO 35_ENT PO9_CC

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Dominio: adquisición e implementación (AI)

De este dominio AI Adquisición e Implementación se seleccionaron los procesos AI3 Adquirir y Mantener Infraestructura Tecnológica, AI5 Adquirir Recursos de TI, AI6 Administrar Cambios, para ser evaluados, donde se identifican los riesgos encontrados.

- ✓ **AI3 Adquirir y mantener infraestructura tecnológica:** los hallazgos o no conformidades encontradas se muestran así:

¡Siempre cerca de Usted !	**HALLAZGOS**	**REF** PLAN AI3_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA** 1 **DE** 2
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones servidores y equipos de cómputo.	
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición Implementación(AI)	**PROCESO**	Adquirir y Mantener Infraestructura tecnológica (AI3)	

HALLAZGO	No hay planos de red de datos de todas las sedes.

RECOMENDACIONES

- Se recomienda que Emssanar ESS levante planos de red de cableado estructurado, para voz datos, corriente normal y regulada, es muy importante proveerse de planos de todos los pisos de todas las sedes interconectadas, en los que se detallen:

  - Ubicación de los gabinetes de telecomunicaciones
  - Ubicación de ductos a utilizar para cableado vertical
  - Disposición detallada de los puestos de trabajo
  - Ubicación de los tableros eléctricos en caso de ser requeridos
  - Ubicación de piso ductos si existen y pueden ser utilizados
  - Tener un diagrama de red que permita identificar fácilmente la localización de puntos y equipos en caso de presentarse problemas en la Red.

- Así mismo deberá mantener actualizado los planos de red, donde se identifiquen los cambios o expansión de red que se realicen.

- El que Emssanar tenga a la mano diseños del cableado estructurado facilitara la administración sencilla y sistemática de los traslados del sitio de trabajo de las personas y equipos. La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, patch panel, armarios de telecomunicaciones y otros espacios ocupados por los sistemas. La norma TIA/EIA 606 proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

¡Siempre cerca de Usted !

HALLAZGOS	REF
	PLAN AI3_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición Implementación(AI)	**PROCESO**	Adquirir y Mantener Infraestructura tecnológica (AI3)		

IMPACTO	• El no contar con planos de red, en el caso de presentarse fallas en la red, impide que se localice de manera inmediata el punto de fallo, implicando pérdida de tiempo y mayores gastos, teniendo en cuenta que los costos en materiales, mano de obra e interrupción de labores al hacer la búsqueda o hacer cambios en el cableado horizontal pueden ser muy altos. • Para la instalación de la red antes se debe realizar el diseño de esta, y se debe tener toda la documentación de los planos, sin embargo el no tenerlos hace que la empresa tenga que contratar personal experto y calificado para el levantamiento de la información y el diseño de la Red, implicando mayores gastos financieros.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

EVIDENCIAS	ANEXO 38_ENT AI3_SP_2

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

¡Siempre cerca de Usted !

HALLAZGOS	REF
	PLAN AI3_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**1 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación (AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO	En Emssanar ESS no existe documentación de la Gestión de red de comunicaciones. (SP)

RECOMENDACIONES

El área de sistemas debe contar con un documento de gestión de red, el cual permita:

- Identificar objetivos encaminados a la monitorización del tráfico y la calidad de servicio.
- Pautas que permitan prevenir, diagnosticar y resolver problemas de la Red.
- Identificación de los usuarios de la red y el software.
- Dar Soporte a los usuarios.
- Pautas de Seguridad
- Gestión de los fallos producidos en la red
- Gestión de rendimiento
- Planificación

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

¡Siempre cerca de Usted !

HALLAZGOS

REF
PLAN AI3_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación (AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

IMPACTO	• El no contar con un documento de gestión de red impide prevenir, diagnosticar y resolver problemas de la red. • La falta de un documento de gestión de red hace que de llegar a ocurrir fallas en la red y hubiese un cambio de personal de gestión de red, causaría un entorno poco fiable, inseguro y difícil de operar ya que no tendría criterios establecidos a seguir.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

EVIDENCIAS	ANEXO 38_ENT AI3_SP_2

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

- ✓ **AI5 Adquirir recursos de TI:** en este proceso no se encontraron hallazgos.

- ✓ **AI6 Administrar cambios:** en este proceso no se encontraron hallazgos.

Dominio: Dar soporte y servicio (DS)

De este dominio DS dar soporte y servicio se seleccionaron los procesos DS4 garantizar la continuidad del servicio, DS8 administrar la mesa de servicio y los incidentes, DS12 administración del ambiente físico. Para ser evaluados cada uno de los procesos están agrupados donde se identifican los riesgos encontrados.

- ✓ **DS4 Garantizar la continuidad del servicio:** en este proceso no se encontraron hallazgos.

- ✓ **DS8 Administrar la mesa de servicio y los incidentes:** en este proceso no se encontraron hallazgos.

- ✓ **DS12 Administración del ambiente físico:** los hallazgos o no conformidades encontradas se muestran en la siguiente página.

¡Siempre cerca de Usted!	**HALLAZGOS**	**REF** PLAN DS12_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA** **1** **DE** **2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.	
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración del ambiente Físico (DS12).	

HALLAZGO	En Emssanar ESS, en cuanto a las condiciones físicas el espacio donde se encuentran ubicados los servidores no está bien adecuado y en la Fundación Emssanar el espacio donde se encuentran ubicados los equipos de computo es limitado no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura, posición de las columnas). (SP, FE)

RECOMENDACIONES

Es importante que el espacio donde se encuentran ubicados los servidores y equipos de computo cuente con las siguientes características : – Debe ser un sitio apropiado en cuanto a la altura mínima libre recomendada del cielo raso es de 2.6 metros, debe contar con un espacio adecuado donde se pueda circular fácilmente. – Paredes lo suficientemente rígidas para soportar los equipos. – Los cuartos de telecomunicaciones donde están ubicados los servidores, deben ser diseñados y aprovisionados de acuerdo a los requerimientos de la norma EIA/TIA 569A. – En cuanto a espacios y movilidad deben ser diseñados y provisionados de acuerdo a la norma ANSI/TIA/EIA-569-A (Normas de recorridos y espacios de Telecomunicaciones en edificios Comerciales), que brinde la posibilidad de movilidad de las personas ya que en algunas oficinas hay espacios limitados.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS

REF
PLAN DS12_3_1

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				2	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración del ambiente Físico (DS12).			

IMPACTO	• El espacio donde se encuentran los servidores y equipos de comunicaciones al no contar con un buen ambiente físico (Movilidad y espacio) en caso de presentarse una emergencia dificulta la evacuación del personal. • La falta de espacio en una oficina o en donde estén ubicados los equipos de cómputo hace que el personal que labora allí no cuente

	con la seguridad con suficientes condiciones laborales, generando estrés e incomodidad laboral.

PROBABILIDAD – IMPACTO			
Probabilidad	Medio	**Impacto**	Medio

EVIDENCIAS	ANEXO 23_ DS12_2_SP ANEXO 26_ DS12_2_FE

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS

REF

PLAN DS12_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				1	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración del ambiente Físico (DS12).			

HALLAZGO	En la sede EPS Emssanar Zonal Ipiales hay ubicación inadecuada de los equipos de comunicación (Modem, Servidor, Patch panel).

RECOMENDACIONES

- En la sede EPS Emssanar Zonal Ipiales los equipos activos (switche, router, etc) deben acogerse a la norma ANSI/TIA/EIA-569-A (Normas de recorridos y espacios de Telecomunicaciones en edificios Comerciales).

- Los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

- Las condiciones físicas donde se encuentran los equipos activos deben cumplir con los requerimientos como:

  - Espacio y movilidad, posibilidad de movilidad de los equipos, características adecuadas del espacio de los equipos, altura, anchura y ubicación de estos.

IMPACTO	• Los equipos activos (switches, router, etc) así como los cables quedan expuestos completamente al polvo y humedad, provocando daños y/o pérdidas de equipos. • Los equipos activos están expuestos a caídas, por estar en el mismo espacio de las oficinas de atención al cliente, las conexiones en los equipos o en el panel de empalme pueden ser manipuladas por cualquier persona. • El daño o pérdida de algún equipo activo genera pérdida de información o el cambio de equipos por consiguiente gastos para remplazar equipos.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_2

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2 DE 2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración del ambiente Físico (DS12).		

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Medio

EVIDENCIAS	IMG_DS12_0001 - IMG_DS12_0002 - IMG_DS12_0003

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S.
¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_2

REF	IMG_DS12_0001

REF	IMG_DS12_0002

REF	IMG_DS12_0003

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

HALLAZGOS	REF
	PLAN DS12_3_3

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			PAGINA 1 DE 3
AREA AUDITADA	Sistemas	OBJETO DE ESTUDIO	Hardware de comunicaciones servidores, y equipos de cómputo.	
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Dar Soporte y Servicio (DS)	PROCESO	Administración de Ambiente Físico (DS12)	

HALLAZGO	En Emssanar ESS, el diagrama de Red Eléctrica no está actualizado, en la Fundación Emssanar no hay red eléctrica segura, los computadores, se conectan directamente tampoco hay suficientes reguladores, en la sede IPS Lorenzo la instalación eléctrica y suministro de energía no es adecuada (No hay polo a tierra) y en la sede EPS Emssanar Zonal Ipiales el tendido de cable no se acoge a las normas EIA/TIA-568 (Canaleta en el piso, cables sueltos, canaletas abiertas).

RECOMENDACIONES

- Es muy importante tener un diagrama de red eléctrica actualizado donde se identifiquen los cambios que se han realizado últimamente o si no se han realizado cambios que se deje observaciones de ello, un diagrama actualizado facilita realizar mantenimiento oportuno, permite vigilar variables de riesgo y elaborar informes de desempeño.

- Las sedes Fundación Emssanar, IPS Lorenzo y EPS Emssanar zonal Ipiales deben cumplir con los requerimientos mínimos del cableado estructurado y de telecomunicaciones, se recomienda hacer una instalación independiente regulada para la conexión de los equipos con base a la norma NTC2050, también que se acoja a la norma EIA/TIA 568, así:

- Debe hacer una revisión de las áreas de trabajo de tal forma que estas estén diseñadas para cambios, modificaciones y adiciones fáciles.

- Debe contar con una infraestructura uniforme de cableado para reducir costos de instalación y mantenimiento.

IMPACTO	• El no tener un diagrama de red eléctrica actualizado no solo conlleva a ignorar cambios que se pudieron haber realizado, también puede ocasionar accidentes catastróficos pues impide ver donde puede estar fallando la red y realizar su mantenimiento preventivo.

RECOMENDACIONES
• Debe existir un plano de red que permita identificar cualquier problema que afecte los procesos que se presenten en esta sede. • Se debe realizar de manera urgente el mantenimiento de la red eléctrica, que permita revisión de los cables salidos de las canaletas o implementar una nueva instalación bien estructurada, en caso contrario adecuar las instalaciones existentes para cumplir con los requerimientos necesarios que garanticen la seguridad física y lógica de los recursos TI. • Verificar que toda la instalación este a su vez conectada a la tierra del edificio, debe existir un sistema de protección en caso de falla del fluido eléctrico como es el caso de UPS y puestas a Tierra. • Utilizar sistemas de alimentación ininterrumpida, que permitan evitar una catástrofe y de esta manera corregir las deficiencias de la red eléctrica. • Se debe garantizar la seguridad de la red eléctrica al personal estas sedes.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_3

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				3	**DE**	**3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones servidores, y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12)			

IMPACTO	• Al presentarse en la sede problemas de infraestructura de red, canaletas abiertas, cables sueltos, red eléctrica tendida en el piso, se podría generar accidentes a quienes laboran en los puestos de trabajo. Se corren riesgos importantes, incluso la electrocución, ya que los problemas eléctricos generan problemas intermitentes difíciles de diagnosticar, provocando deterioros importantes en los dispositivos de red incluso generando daños y mal funcionamiento frecuente en los equipos de computo y comunicación. • La insuficiencia de reguladores hace que algunos equipos se conecten directamente a la energía, exponiendo a los equipos a picos altos y bajos de energía que si bien conocemos esto generaría equipos quemados o daños irreversibles de gran parte del hardware, provocando gastos mayores. • La deficiencia de la red eléctrica no garantiza la seguridad de las personas y los equipos en caso de presentarse algún accidente.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

EVIDENCIAS	– ANEXO 42_ENT DS12_SP_2 – ANEXO 44_ENT_DS12_FE_1 – ANEXO 47_ENT_DS12_LZ_1 – **IPI ➔** IMG_DS12_0004 - IMG_DS12_0005 - IMG_DS12_0006 - IMG_DS12_0007 - IMG_DS12_0008

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S.
¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_3

REF	IMG_DS12_0004

REF	IMG_DS12_0005

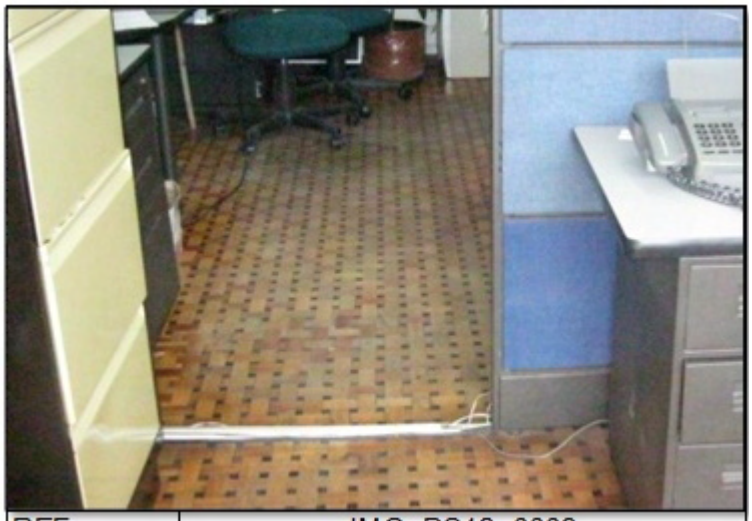
REF	IMG_DS12_0006

Emssanar E.S.S.
¡Siempre cerca de Usted!

HALLAZGOS

REF
PLAN DS12_3_3

REF	IMG_DS12_0007



REF	IMG_DS12_0008

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S.
¡Siempre cerca de Usted !

HALLAZGOS	REF
	PLAN DS12_3_4

HALLAZGO	En las sede Oresemillas la seguridad del cuarto de comunicaciones o Rack no sigue las normas de seguridad establecidas en el estándar ANSI/TIA/EIA-569.			**PAGINA** 1 **DE** 2
ENTIDAD AUDITADA	E.S.S. - Nariño			
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.	
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).	

HALLAZGOS	**REF**
MENDA	PLAN DS12_3_4

- Se recomienda definir un espacio adecuado para el lugar donde esta instalado el cuarto de comunicaciones que se ajuste a las normas de seguridad.
- Se recomienda área exclusiva para el equipo de comunicaciones en este caso para el armario de comunicaciones donde según el estándar ANSI/TIA/EIA-569 se debe tener en cuenta:
  - Libre de HVAC (Humedad, Ventilación, Aire Acondicionado y Calefacción).
  - Seguridad para personas no autorizadas, se debe mantener el cuarto de telecomunicaciones con llave en todo momento. Se debe asignar llaves únicamente al personal encargado o autorizado que esté en la sede durante las horas de operación.
  - Se debe mantener el cuarto de telecomunicaciones limpio y ordenado.
  - Buena iluminación, se recomienda tener luces de emergencia por si al foco se daña.
  - Se recomiendan no tener cables sueltos dentro del armario, utilizar amarres o cintillas tipo Velcro.
  - Se debe evitar polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática.
  - Se debe evitar el uso de cielos falsos en los cuartos de telecomunicaciones.
- Teniendo en cuenta que el espacio donde está ubicado el Rack es extremadamente grande, acondicionar parte del espacio para ubicar el rack teniendo en cuenta las medidas adecuadas y que se ajuste a la norma para proteger los recursos que forman parte de los equipos de comunicación.

- Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) del cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2** **DE** **2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).		

RECOMENDACIONES
• Realizar mantenimiento periódico a los cuartos de comunicación.

IMPACTO	• El espacio donde está ubicado el cuarto de comunicaciones es muy grande, el techo es de eternit y tiene escapes de aire, lo cual hace que la entrada de polvo sea libre perjudicando los equipos de comunicación. • Los cables sueltos y la desorganización de estos hacen que no cumpla con la ANSI/TIA/EIA-569, esto hace que la distribución del cableado no sea ordenada ocasionando daños e interrupciones o atenuación de la Red, generando mal funcionamiento de desempeño de la Red. • Por ser un salón grande donde está ubicado el rack de comunicaciones hace que a este no se le dé la importancia de cómo este debe mantenerse, ya que este lugar se presta para guardar objetos diferentes a lo que tiene que ver con equipos de comunicación o muchas veces se lo tome como bodega para guardar tubos y sobrantes de estos.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Medio

EVIDENCIAS	IMG_DS12_0009 IMG_DS12_0010 IMG_DS12_0011 IMG_DS12_0012

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

REF	IMG_DS12_0009

REF	IMG_DS12_0010

REF	IMG_DS12_0011

REF	IMG_DS12_0012

HALLAZGO	En la sede CooEmssanar IPS la red eléctrica no es segura por falta de UPS y reguladores y en la sede Laboratorio Clínico Emssanar no hay generadores de corriente si se fuese la energía.					
RECOMENDACIONES	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
ENTIDAD AUDITADA				**1**	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones (Red Eléctrica)			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).			

- La sede CooEmssanar IPS y Laboratorio Clínico Emssanar deben cumplir con los requerimientos mínimos del cableado estructurado y de telecomunicaciones, según la norma EAI/TIA 568, así:
- Debe contar con una infraestructura uniforme de cableado para reducir costos de instalación y mantenimiento.
- Debe existir un plano de red que permita identificar cualquier problema que afecte los procesos que se presente en esta sede.

- Debe haber suficientes reguladores o ups que soporte el número que equipos de trabajo.

- En las dos sedes por la función que desempeña y los equipos que estas sedes utilizan para prestar el servicio a usuarios, deben contar con la seguridad de que en dado caso en que llegase a irse la energía puedan contar con un suministro como generador de corriente ininterrumpida que les permita terminar dicha acción que se esté ejecutando y no cancelarse repentinamente.
- Seleccionar una empresa para la compra de este equipo que ofrezca la instalación, mantenimiento y reparación. Esto es importante ya que se planea tener una fuente de energía que esté listo para salir en cualquier emergencia. El equipo tiene que ser probado por lo menos trimestralmente.

¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_5

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				2	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de Comunicaciones (Red Eléctrica)			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).			

IMPACTO	• La deficiencia de la red eléctrica no garantiza la seguridad de las personas y los equipos, provocando que se presenten graves accidentes como incendios a causa de presentarse sobrecarga eléctrica.

	• La instalación y suministro de energía no es la adecuada para estas sedes, provocando daños en los equipos de cómputo más frecuentes. • La insuficiencia de reguladores hace que algunos equipos se conecten directamente a la energía, exponiendo a los equipos a picos altos y bajos de energía que si bien conocemos esto generaría equipos quemados o parte del hardware dado de baja. • Un apagón de energía por un largo periodo podría poner en peligro el funcionamiento de esta sede y generar un alto coste financiero, ya que se puede perder información, datos, resultados de laboratorio, tiempo, etc.

PROBABILIDAD – IMPACTO			
Probabilidad	Bajo	**Impacto**	Alto

EVIDENCIAS	ANEXO 43_ENT_DS12_E.IPS ANEXO 46_ENT_DS12_LAB

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_6

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	
				1	**DE** **3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).		

HALLAZGO	En Emssanar ESS, el espacio donde se encuentran ubicados los servidores no cuenta con materiales incombustibles (Pintura de las paredes, suelo, techo, mesas, etc), no existe protección contra incendios ni otros peligros físicos que en dado caso pueden afectar el espacio

	donde se encuentran ubicados los servidores (SP) y en las sedes SIAU Y EPS Emssanar zonal Ipiales y en Atención al Usuario Emssanar Córdoba no hay extintor.

RECOMENDACIONES

- Emssanar ESS debe contar con un sistema de protección contra incendios de todo el edificio, con el fin de salvar vidas humanas, minimizar las pérdidas económicas producidas por el fuego, conseguir que las actividades del edificio puedan reanudarse en el menor tiempo posible, entre otras.
- Es importante que el espacio donde se encuentran ubicados los servidores cuente con paredes lo suficientemente rígidas para soportar los equipos, utilizando pintura resistente al fuego, lavable, mate y de color claro.
- El no contar con materiales incombustibles hace que si llegase a ocurrir un accidente en este caso un incendio nada impedirá que se retarden su inflamación, convirtiéndose esto en un desastre catastrófico.
- Realizar una evaluación de todas las sedes en cuanto a seguridad de establecimientos o sedes en este caso con el fin de disponer del número total de extintores indicado en el plan de protección y evacuación del centro de trabajo para proteger la seguridad del personal y evitar riesgos inesperados.
- Cumplir con las revisiones periódicas reglamentarias que garanticen seguridad de establecimientos o sedes en este caso. Cada año hay que comprobar el peso y la presión de la carga en el caso de los extintores, así como realizar una inspección ocular de su estado general. Cada año, a partir de la fecha que conste en el exterior del extintor, cargarlo de nuevo.

Emssanar E.S.S. ¡Siempre cerca de Usted!

HALLAZGOS

REF
PLAN DS12_3_6

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**2** **DE** **3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores y equipos de computo		
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).		

RECOMENDACIONES

• Cada tres meses, la propia empresa o una contratada de mantenimiento debe hacer una inspección ocular de la conservación del extintor (partes mecánicas, precintos, inscripciones), así como comprobar su correcta accesibilidad y señalización, así mismo instalar los extintores en lugares visibles y accesibles, próximos a puntos con riesgo de incendio y a las salidas de evacuación. Se instalarán, preferiblemente, sobre soportes fijados verticales, como máximo, a 1,70 metros del suelo. • Capacitar a todo el personal del centro de trabajo sobre los conocimientos básicos del fuego y en el manejo de los extintores.

IMPACTO	• El impacto que ocasiona el no contar con materiales incombustibles y no tener un sistema contraincendios en la sede principal donde se encuentran ubicados los servidores, si se presentase un accidente provocado por el fuego habría cese de actividades, pérdidas económicas y desastres catastróficos. • El que no haya un extintor en una oficina, donde se sabe que se trabaja utilizando diferentes equipos conectados a energía hace que se presente en las sedes o en la empresa como tal factores de riesgo que inciden en el buen funcionamiento empresarial creando falencias bajas que se pueden convertir en graves si llegasen a ocurrir. • El no hacerles el respectivo mantenimiento a los extintores causaría que estos estén en la empresa pero vencidos y quizá en caso de presentarse un incendio lo que genere sea un accidente fatal de la persona que lo manipule en ese momento.

PROBABILIDAD – IMPACTO	Empresa Solidaria De Salud EMSSANAR				**PAGINA**		
ENTIDAD AUDITADA	E.S.S – Nariño				**3**	**DE**	**3**
Probabilidad	Medio		**Impacto**	Alto			
AREA	Sistemas	**OBJETO DE**	Hardware de comunicaciones,				
AUDITADA		**ESTUDIO**	servidores y equipos de computo				
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.						
MATERIAL DE SOPORTE	COBIT						
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).				

EVIDENCIAS	ANEXO 41_ENT DS12_SP_1 ANEXO 27_DS12_2_SIAU

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Emssanar E.S.S.
¡Siempre cerca de Usted!

HALLAZGOS	**REF**
	PLAN DS12_3_7

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				1	**DE**	**2**
HALLAZGO	En Emssanar ESS, no existen sistemas de alarmas, ni cámaras de seguridad, ni detección de movimiento, en la sede Fundación Emssanar [illegible] no hay señalización [illegible] las sedes Laboratorio Clínico y en IPS Lorenzo no hay seguridad de vigilancia.					
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).			

RECOMENDACIONES

- La seguridad en un cuarto de comunicaciones es primordial debido a los riesgos que se pueden presentar como robos [illegible] los recursos de TI, cámaras de seguridad es uno de los aparatos más populares que se puede utilizar, una cámara no puede parar a nadie de robar, pero si ofrece tranquilidad y seguridad, lo mismo que un sistema de alarma, colocado en un sitio estratégico, puede detectar fácilmente la presencia de extraños lo cual evitaría que los equipos estén en riesgo o peor aun la perdida de información.
- Las instalaciones de la Fundación Emssanar dentro de los objetivos deberá proporcionar unas orientaciones básicas para facilitar el proceso de la señalización relativa a las situaciones y actuaciones de emergencia, esto con el fin de garantizar la seguridad y salud de los trabajadores. Esta señalización abarcara tanto la señalización de la localización de los medios de protección contra incendios como la señalización de evacuación, salvamento y socorro en sus diferentes tipos y modalidades.
- Todas las sedes deben acogerse a la normativa y normas técnicas relacionadas con prevención de riesgos laborales, disposiciones mínimas en materia de señalización de seguridad y salud en el trabajo, disposiciones mínimas de seguridad y salud en los lugares de trabajo, etc.
- La sede IPS Lorenzo por ser una de las sedes que prestan atención al usuario y como tal atiende un gran número de usuarios se debe implementar medidas de seguridad para el acceso a la entidad, debe existir una persona encargada de la seguridad de la sede.
- En las sedes Laboratorio Clínico Emssanar y en IPS Lorenzo se debe establecer medidas de seguridad que permitan garantizar seguridad tanto del personal como de los recursos TI de la sede y se debe tener en cuenta lo siguiente:
  - Control de la entrada y salida de las instalaciones de estas sedes (Identificación de todo individuo que ingresa).

Emssanar E.S.S. ¡Siempre cerca de Usted !

HALLAZGOS	**REF**
	PLAN DS12_3_7

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**		
				2	**DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Hardware de comunicaciones, servidores, y equipos de cómputo.			
RESPONSABLES	Laura Yaneth Noguera Q. y Edy Yanira Sánchez P.					
MATERIAL DE SOPORTE	COBIT					
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).			

RECOMENDACIONES

- Realizar requisas a las personas que ingresan y salen de las instalaciones.
- Registro de equipos de cómputo, portátiles que ingresan y que salen de las sedes.

IMPACTO	• El que no haya cámaras de seguridad, alarmas, ni detectores de movimiento, impide evitar robos o ataques contra los activos de la empresa. • El que no haya señalización de evacuación en caso de presentarse una emergencia genera diferentes tipos de problemas a la cual la empresa queda expuesta por hacer caso omiso a esta recomendación. • En caso de presentarse, la sede queda expuesta a una investigación exhaustiva permitiendo identificar situaciones de riesgo desconocidas o poco favorables o quizá innecesarias. • Un vigilante de seguridad es la persona encargada de proteger la integridad física de las personas y los bienes materiales de la empresa donde labora, razón por la cual si no lo hay en un de estas sedes, se presenta inseguridad tanto del personal como de los bienes que en ella existen, causando inestabilidad laboral y material, en este caso en Laboratorio y en IPS Lorenzo. • El ingreso de personas mal intencionadas genera inestabilidad e inseguridad a los usuarios (pacientes).

PROBABILIDAD – IMPACTO			
Probabilidad	Medio	**Impacto**	Alto

EVIDENCIAS	ANEXO 41_ENT DS12_SP_1 ANEXO 26_DS12_2_FE ANEXO 25_DS12_2_LAB ANEXO 29_DS12_2_LZ

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

Dominio: monitorear y evaluar (ME)

De este dominio ME monitorear y evaluar, se seleccionaron los procesos me1 monitoreo y evaluación de desempeño de TI, ME2 monitoreo y evaluación de control interno para ser evaluados, donde se identifican los riesgos encontrados.

- ✓ **Monitoreo y evaluación de desempeño de TI (ME1):** en este proceso no se encontraron hallazgos.

- ✓ **Monitoreo y evaluación de control interno (ME2):** en este proceso no se encontraron hallazgos.

2.3.8 Informe general de la auditoría

Objetivos

Realizar la auditoria en la empresa solidaria de salud Emssanar E.S.S en el área de sistemas, con el fin de identificar vulnerabilidades en cuanto al hardware de comunicaciones, servidores y equipos de computo e Indicadores de funcionamiento, con respecto a mantenimiento, soporte, adquisición de hardware, inventarios, administración de cambios, funcionamiento del hardware; a nivel central (sede principal Pasto), zonal (Ipiales) y a nivel municipal (Córdoba).

Objetivos específicos

- Identificar cada uno de los procesos y procedimientos correspondientes al hardware de las comunicaciones, servidores, equipos de cómputo e indicadores del área de sistemas de la Empresa EMSSANAR E.S.S.
- Identificar debilidades y fortalezas en la parte física de las comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento.
- Identificar cada uno de los 4 campos tomados como caso de estudio y proceder a realizar la auditoria en cada uno de ellos.
- Analizar el funcionamiento de las comunicaciones en cuanto a proveedores, contratos y soporte.
- Analizar el funcionamiento de los servidores en cuanto a garantías, instalaciones, respaldos, políticas de contingencia, políticas de seguridad y políticas de mantenimiento.
- Verificar el cumplimiento de los indicadores de funcionamiento en los niveles de cobertura, de obsolescencia, de soporte tecnológico y tiempo fuera de servicio.

Limitaciones

No se tuvo acceso a alguna información clave en cuanto al Hardware de comunicaciones, como planos de red, inventario de hardware de equipos de comunicaciones, lo que impidió diagnosticar el proceso de normas y certificación de puntos de la red montada en la sede central de Nariño.

Por lo demás la auditoría se realizó de forma adecuada según el área auditada, donde se aplicaron diferentes entrevistas y cuestionarios contando con total colaboración del jefe de Sistemas y personal del área de sistemas de Emssanar E.S.S.

Resultados obtenidos de la auditoria

A continuación se describen los hallazgos encontrados en cada uno de los procesos evaluados en el área de sistemas de Emssanar E.S.S con sus respectivas recomendaciones claves que permitirá a la empresa definir planes de mejoramiento. De acuerdo a los procesos de COBIT auditado. Tenemos:

DOMINIO COBIT - PLANIFICACION Y ORGANIZACIÓN (PO)

Proceso COBIT PO3: Determinar la dirección tecnológica

Hallazgo

En Emssanar ESS, el plan de contingencia en caso de que el hardware no funcione no está documentado. (Ver ANEXO 32_ENT PO3_SP).

Recomendaciones

En la empresa debe existir un documento de plan de contingencia que permita dar solución inmediata en caso de presentarse algún fallo en el hardware.

El documento del plan de contingencia debe contener:

- Objetivos claros para restaurar los servicio de forma rápida, eficiente y con el menor costo y pérdidas posibles.
- Pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del los servicios.
- Estrategias para la recuperación de desastres.

En cuanto a los diferentes niveles de daños, también se hace necesario presuponer el daño total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Proceso COBIT PO9: Evaluación de riesgos

Hallazgos

- En Emssanar E.S.S no hay políticas o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones. (Ver ANEXO 33_ENT_PO9_SP).

- En la fundación Emssanar y en la IPS Lorenzo existen problemas con conectividad, con baja velocidad, bloqueo y limitación de accesos a internet. (Ver ANEXO 34_ENT PO9_FE y ANEXO 36_ENT PO9_LZ).

- En las sedes Fundación Emssanar y en Cresemillas en la dependencia de Centro de Contactos existe deficiencia en cuanto al mantenimiento físico de los equipos y actualizaciones de programas de Antivirus. (Ver ANEXO 34_ENT PO9_FE y ANEXO 35_ENT PO9_CC).

Recomendaciones

- En Emssanar EPS debe existir un procedimiento que permita realizar el análisis y la

gestión de riesgos para el funcionamiento del hardware de las comunicaciones, los equipos de cómputo y los servidores.

- Es fundamental tener un método para realizar la gestión de riesgos que se integre dentro de la gestión de diferentes proyectos y que así mismo el equipo del proyecto esté involucrado en la identificación y seguimiento de los riesgos.

- Es importante que Emssanar ESS cuente con una herramienta que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del control informático.

- En Las sedes Fundación Emssanar y en la IPS Lorenzo continuamente se debe revisar el cronograma de mantenimiento o funcionamiento de la red, sobre todo en estas sedes, ya que el uso de internet es necesario para la implementación de diferentes proyectos que se desarrollan y así mismo no afectar el buen funcionamiento de estas.

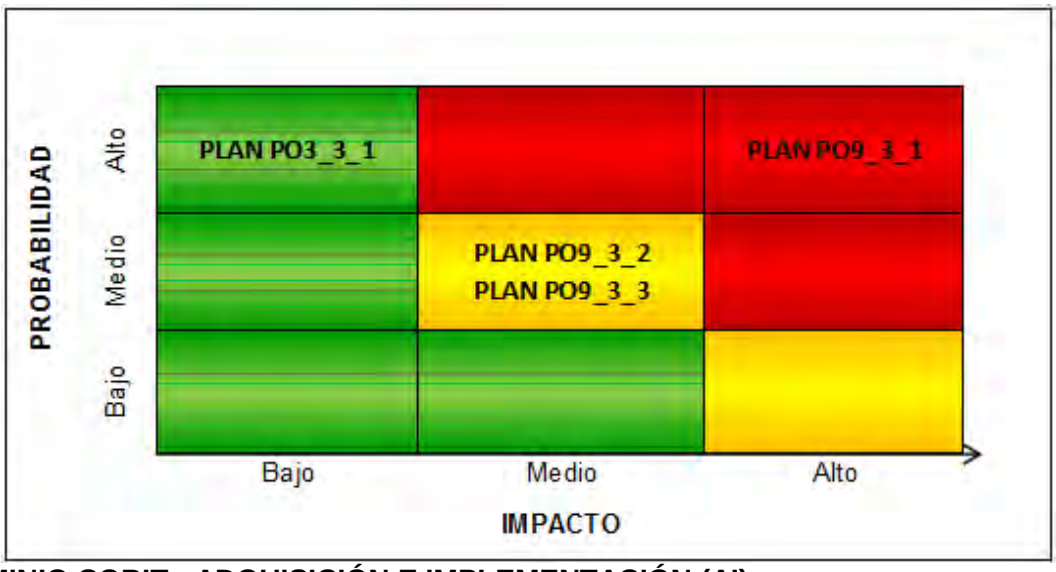
- Se debe hacer un estudio más detallado de las sedes y del personal para priorizar que módulos o que funcionarios deben tener acceso a trabajar con mayor velocidad de internet, de a cuerdo a la función que desempeñen.

- Actualizar permanentemente el Programa de Antivirus.

- El desarrollo del mantenimiento se efectuara en conformidad con un cronograma establecido, el mismo será coordinado con los funcionarios a fin de tener toda la disponibilidad de los equipos sin afectar sus labores cotidianas.

- El mantenimiento preventivo y correctivo es importante hacerlo frecuentemente en estas sedes, muy importante visitar las sedes periódicamente que permita hacer una evaluación del comportamiento de todo lo que tiene que ver con el funcionamiento del hardware y actualizaciones de software que responda a las necesidades del trabajo.

Matriz de probabilidad e impacto



DOMINIO COBIT - ADQUISICIÓN E IMPLEMENTACIÓN (AI)

Proceso COBIT AI3: adquirir y mantener infraestructura tecnológica hallazgos

- No hay planos de red de datos de todas las sedes. (Ver ANEXO 38_ENT AI3_SP_2).
- En Emssanar ESS no existe documentación de la Gestión de red de comunicaciones. (Ver ANEXO 38_ENT AI3_SP_2).

Recomendaciones

- Se recomienda que Emssanar ESS, levante planos de red de cableado estructurado, para voz datos, corriente normal y regulada, es muy importante proveerse de planos de todos los pisos de todas las sedes interconectadas, que permita identificar fácilmente la localización de puntos y equipos en caso de presentarse problemas en la red.

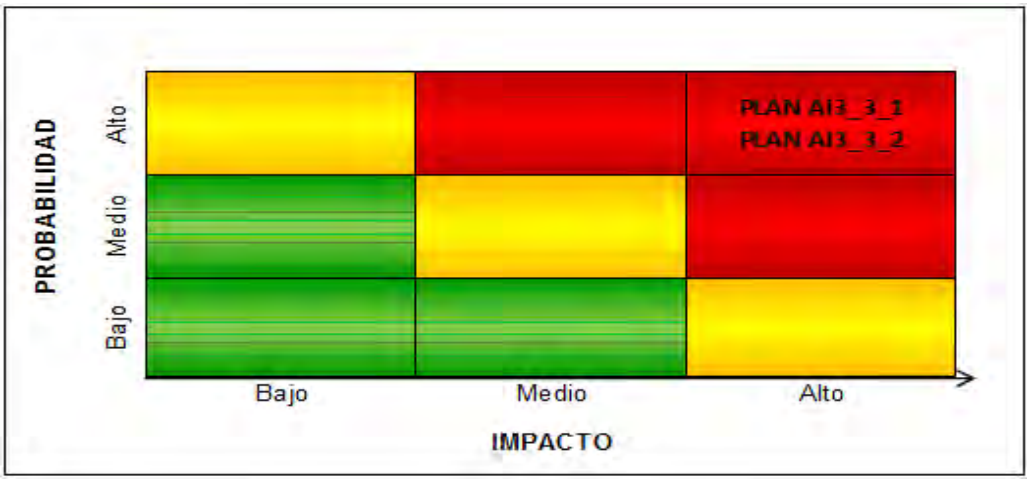
- Así mismo deberá mantener actualizado los planos de red, donde se identifiquen los cambios o expansión de red que se realicen.

- El que Emssanar tenga a la mano diseños del cableado estructurado facilitara la administración sencilla y sistemática de los traslados del sitio de trabajo de las personas y equipos. La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, patch panel, armarios de telecomunicaciones y otros espacios ocupados por los sistemas. La norma TIA/EIA 606 proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.

- El área de sistemas debe contar con un documento de gestión de red, que permita identificar objetivos encaminados a la monitorización del tráfico y la calidad de servicio, pautas que permitan prevenir, diagnosticar y resolver problemas de la red, identificación de los usuarios de la red y el software, dar Soporte a los usuarios,

gestión de los fallos producidos en la red, gestión de rendimiento, planificación, etc.

Matriz de probabilidad e impacto.



DOMINIO COBIT - DAR SOPORTE Y SERVICIO (DS)

Proceso COBIT DS12: administración del ambiente físico

Hallazgos

- En Emssanar ESS en cuanto a las condiciones físicas el espacio donde se encuentran ubicados los servidores no está bien adecuado y en la Fundación Emssanar el espacio donde se encuentran ubicados los equipos de computo es limitado no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura, posición de las columnas). (Ver ANEXO 23_ DS12_2_SP, ANEXO 26_ DS12_2_FE).

- En la sede EPS Emssanar Zonal Ipiales hay ubicación inadecuada de los equipos de comunicación (modem, servidor, patch panel). (Ver IMG_DS12_0001, IMG_DS12_0002, IMG_DS12_0003).

- En Emssanar ESS, el diagrama de red eléctrica no está actualizado. (Ver ANEXO 42_ENT DS12_SP_2,

- En la Fundación Emssanar no hay red eléctrica segura, los computadores, se conectan directamente tampoco hay suficientes reguladores. (Ver ANEXO 44_ENT_DS12_FE_1).

- En la sede IPS Lorenzo la instalación eléctrica y suministro de energía no es adecuada. (No hay polo a tierra). (Ver ANEXO 47_ENT_DS12_LZ_1).

- En la sede EPS Emssanar zonal Ipiales, el tendido de cable no se acoge a las normas EIA/TIA-568. (Canaleta en el piso, cables sueltos, canaletas abiertas). (Ver.

IMG_DS12_0004, IMG_DS12_0005, IMG_DS12_0006, IMG_DS12_0007, IMG_DS12_0008).

- En las sede Cresemillas la seguridad del cuarto de comunicaciones o Rack no sigue las normas de seguridad establecidas en el estándar ANSI/TIA/EIA-569. (Ver IMG_DS12_0009, IMG_DS12_0010, IMG_DS12_0011, IMG_DS12_0012)

- En la sede CooEmssanar IPS la red eléctrica no es segura por falta de UPS y reguladores. (Ver ANEXO 43_ENT_DS12_E.IPS).

- En la sede Laboratorio Clínico Emssanar No hay generadores de corriente si se fuese la energía. (Ver ANEXO 46_ENT_DS12_LAB).

- En Emssanar ESS, el espacio donde se encuentran ubicados los servidores no cuenta con materiales incombustibles (Pintura de las paredes, suelo, techo, mesas, etc). (Ver ANEXO 41_ENT DS12_SP_1 y ANEXO 27_DS12_2_SIAU).

- En la sede Principal, no existe protección contra incendios ni otros peligros físicos que puedan afectar el espacio donde se encuentran ubicados los servidores. (Ver ANEXO 41_ENT DS12_SP_1 y ANEXO 27_DS12_2_SIAU).
- En las sedes SIAU Y EPS Emssanar zonal Ipiales y en Atención al Usuario Emssanar Córdoba no hay extintor. (Ver ANEXO 41_ENT DS12_SP_1 y ANEXO 27_DS12_2_SIAU).

- En Emssanar ESS, no existen sistemas de alarmas, ni cámaras de seguridad, ni detección de movimiento. (Ver ANEXO 41_ENT DS12_SP_1).

- En la sede Fundación Emssanar no hay señales de evacuación. (Ver ANEXO 26_DS12_FE)

- En las sedes Laboratorio Clínico y en IPS Lorenzo no hay seguridad de vigilancia. (Ver ANEXO 25_DS12_LAB y ANEXO 29_DS12_LZ).

Recomendaciones

- En las instalaciones de la Fundación Emssanar el espacio donde están ubicados los equipos de cómputo debe cumplir con la norma ANSI/TIA/EIA-569-A que brinde la posibilidad de movilidad de las personas ya que en algunas oficinas hay espacios limitados.

- En la sede EPS Emssanar Zonal Ipiales los equipos activos (switche, router, etc) deben acogerse a la norma ANSI/TIA/EIA-569-A (Normas de recorridos y espacios de Telecomunicaciones en edificios Comerciales).

- Emssanar E.S.S debe tener un diagrama de red eléctrica actualizado donde se identifiquen los cambios que se han realizado últimamente o si no se han realizado cambios, que se deje observaciones de ello, un diagrama actualizado facilita realizar mantenimiento oportuno, permite vigilar variables de riesgo y elaborar informes de desempeño.

- Las sedes Fundación Emssanar, IPS Lorenzo EPS, Emssanar zonal Ipiales y la sede Atención al Usuario Emssanar Córdoba deben cumplir con los requerimientos mínimos del cableado estructurado y de telecomunicaciones, Se recomienda hacer una instalación independiente regulada para la conexión de los equipos con base a la norma NTC2050, como también que se acoja a la norma EIA/TIA 568.

- Se debe realizar de manera urgente el mantenimiento de la red eléctrica, que permita revisión de los cables salidos de las canaletas o implementar una nueva instalación bien estructurada, en caso contrario adecuar las instalaciones existentes para cumplir con los requerimientos necesarios que garanticen la seguridad física y lógica de los recursos TI.

- Utilizar sistemas de alimentación ininterrumpida, que permitan evitar una catástrofe y de esta manera corregir las deficiencias de la red eléctrica.
- Se debe garantizar la seguridad de la red eléctrica al personal estas sedes.

- Se recomienda definir un espacio adecuado para el lugar donde está instalado el cuarto de comunicaciones donde se ajuste a las normas de seguridad establecidos según el estándar ANSI/TIA/EIA-569.

- Realizar mantenimiento periódico a los cuartos de comunicación.

- La sede CooEmssanar IPS y Laboratorio Clínico Emssanar deben cumplir con los requerimientos mínimos del cableado estructurado y de telecomunicaciones, según la norma EAI/TIA 568.

- Es importante que el espacio donde se encuentran ubicados los servidores cuente con paredes lo suficientemente rígidas para soportar los equipos, utilizando pintura resistente al fuego, lavable, mate y de color claro.

- Emssanar ESS debe contar con un sistema de protección contra incendios de todo el edificio, con el fin de salvar vidas humanas, minimizar las pérdidas económicas producidas por el fuego, conseguir que las actividades del edificio puedan reanudarse en el menor tiempo posible, entre otras.

- Realizar una evaluación de todas las sedes en cuanto a seguridad de establecimientos o sedes en este caso con el fin de disponer del número total de extintores indicado en el plan de protección y evacuación del centro de trabajo para

proteger la seguridad del personal y evitar riesgos inesperados.

- Capacitar a todo el personal del centro de trabajo sobre los conocimientos básicos del fuego y en el manejo de los extintores.

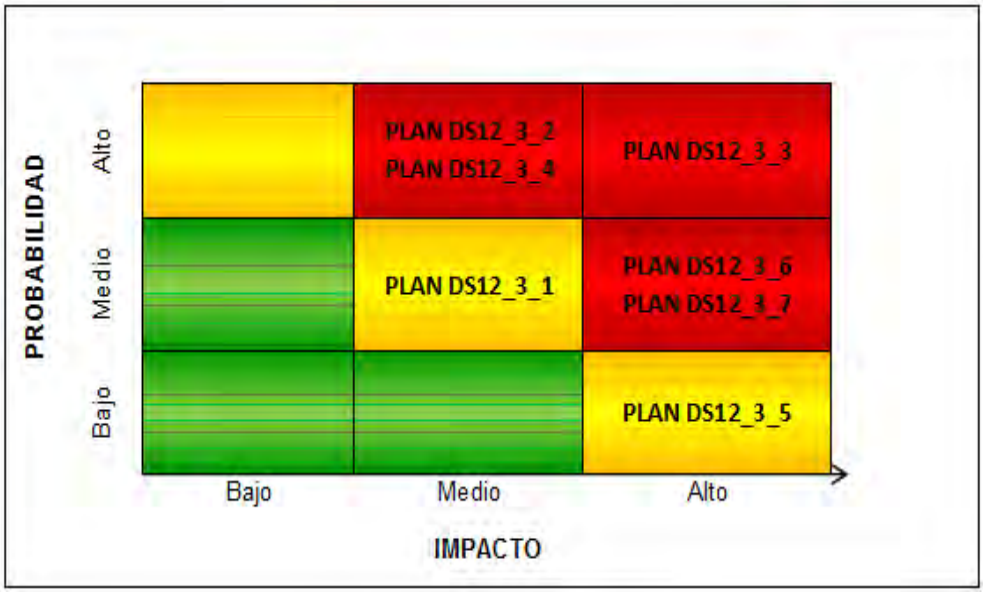
- La seguridad en un cuarto de comunicaciones es primordial debido a los riesgos que se pueden presentar como robos o atentados contra los recursos de TI; cámaras de seguridad es uno de los aparatos más populares que se puede utilizar, una cámara no puede parar a nadie de robar, pero si ofrece tranquilidad y seguridad, lo mismo que un sistema de alarma, colocado en un sitio estratégico, puede detectar fácilmente la presencia de extraños lo cual evitaría que los equipos estén en riesgo o peor aun la perdida de información.

- Las instalaciones de la Fundación Emssanar dentro de los objetivos deberá proporcionar unas orientaciones básicas para facilitar el proceso de la señalización relativa a las situaciones y actuaciones de emergencia, esto con el fin de garantizar la seguridad y salud de los trabajadores. Esta señalización abarcara tanto la señalización de la localización de los medios de protección contra incendios como la señalización de evacuación, salvamento y socorro en sus diferentes tipos y modalidades.

- Todas las sedes deben acogerse a la normativa y normas técnicas relacionadas con prevención de riesgos laborales, disposiciones mínimas en materia de señalización de seguridad y salud en el trabajo, disposiciones mínimas de seguridad y salud en los lugares de trabajo, etc.

- En las sedes Laboratorio Clínico Emssanar y en IPS Lorenzo se debe establecer medidas de seguridad que permitan garantizar seguridad tanto del personal como de los recursos TI de la sede.

Matriz de Probabilidad e Impacto


PROBABILIDAD
Alto
Medio
Bajo
PLAN DS12_3_2
PLAN DS12_3_4
PLAN DS12_3_3
PLAN DS12_3_1
PLAN DS12_3_6
PLAN DS12_3_7
PLAN DS12_3_5
Bajo
Medio
Alto
IMPACTO

2.3.9 Informe ejecutivo de la auditoria

El informe ejecutivo de la Auditoría Informática en el área de sistemas e indicadores de funcionamiento del hardware en la empresa solidaria de salud Emssanar E.S.S del departamento de Nariño se presenta en la siguiente página.

San Juan de Pasto, 24 de mayo del 2012

Ingeniero
HAROLD CAICEDO
Ingeniero de Sistemas
Jefe de Sistemas Emssanar E.S.S Regional Nariño
Ciudad

REF: AUDITORÍA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S DEL DEPARTAMENTO DE NARIÑO.

Cordial saludo,

El presente es el informe de la auditoría a la que fue sometida el área de sistemas, con el objetivo de evaluar los procesos del hardware de comunicaciones, servidores y equipos de cómputo e indicadores de funcionamiento.

Los resultados obtenidos son producto de la aplicación de técnicas y herramientas de auditoría, teniendo como base la información y documentación que fue suministrada por la entidad auditada.

Los resultados obtenidos se sustentan como hallazgos con sus respectivas recomendaciones y en algunos casos fortalezas encontradas. Estos son:

HARDWARE DE COMUNICACIONES

- En Emssanar ESS no hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de las comunicaciones.

  Impacto. La gestión de riesgos permite anticiparse al futuro y prevenir a la empresa de diferentes problemas en este caso riesgos que pongan en peligro el buen funcionamiento de las comunicaciones y el que no hayan políticas o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de las comunicaciones impide hacer una visión a futuro y prevenir a

la empresa de diferentes problemas que se puedan presentar, también implica tomar decisiones inmediata frente a un problema sin tener previo análisis de este ni tener la certeza de poder mitigar ese riesgo, generando altos costos de la gestión por crisis, presencia alta de sorpresas y problemas, perder ventaja competitiva, entre otras.

Recomendación. En Emssanar ESS debe existir un procedimiento que permita realizar el análisis y la gestión de riesgos para el funcionamiento del hardware de las comunicaciones donde se pueda identificar y clasificar los riesgos, determinar la probabilidad de ocurrencia e impacto, identificación de controles que los mitiguen y toma de decisiones frente a esos riesgos, también es importante que en Emssanar dentro del área de sistemas cuente con una herramienta de software que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del control informático.

- No hay planos de red de datos de todas las sedes.

  Impacto. En caso de presentarse fallas, el no contar con documentos de los planos de red, impide que se localice de manera inmediata el punto de fallo, implicando pérdida de tiempo y mayores gastos, teniendo en cuenta que los costos en materiales, mano de obra e interrupción de labores al hacer la búsqueda o hacer cambios en la infraestructura pueden ser muy altos.

  Recomendación. Se recomienda levantar y mantener actualizados los planos de la red de voz y datos de la sede principal y de todas las sedes interconectadas, donde se pueda evidenciar los elementos de la red como gabinetes de telecomunicaciones, puestos de trabajo, puntos de red, cuellos de botella, entre otros, esto con el fin de facilitar la identificación de problemas y sorpresas que se pueden presentar y cambios que se pueden realizar, esto con el fin de facilitar la administración sencilla y sistemática de la red.

- En Emssanar ESS, en el área de sistemas no existe documentación de la Gestión de red de comunicaciones.

  Impacto. El no contar con un documento de gestión de red impide prevenir, diagnosticar y resolver problemas de la red, en caso de ocurrir fallas en la red y hubiese un cambio de personal de gestión de red, causaría un entorno poco fiable, inseguro y difícil de operar ya que no tendría criterios establecidos a seguir.

  Recomendación. Se recomienda que el área de sistemas cuente con un documento de gestión de red, el cual permita identificar objetivos encaminados a la monitorización del tráfico y la calidad del servicio, pautas que permitan

prevenir, diagnosticar y resolver problemas de la red, pautas de seguridad, gestión de los fallos producidos en la red, gestión de rendimiento y planificación y obtener un software de gestión de red que proporcione funciones de gestión y comunicaciones para la operación, administración y mantenimiento de la red de telecomunicaciones y provisionamiento de sus servicios en el entorno en el que se extiende la red.

Fortaleza. El área de sistemas cuenta con personal calificado capaz de monitorear la red, conoce y aplica el proceso de gestión de red, administrando de forma adecuada los recursos con los que cuenta la empresa, con el objetivo de dar continuidad a los servicios que presta a sus usuarios y mantener funcionando correctamente la red como un todo y cada uno de sus elementos individualmente.

- El plan de contingencia en caso de que el hardware no funcione no está documentado.

  Impacto. El no contar con un plan de contingencia dificulta la recuperación de seguir trabajando en un plazo mínimo después de que se haya presentado un problema o desastre inesperado, en caso de presentarse un fallo del hardware la solución de un proceso practico a seguir sería aplicable para un problema técnico y pequeño pero no para un desastre o catástrofe, la interrupción de los servicios de computación y comunicación seria prolongada llevando a las empresa a pérdidas financieras significativas.

  Recomendación. En la empresa debe existir un plan de contingencia documentado que permita dar solución inmediata en caso de presentarse algún fallo en el hardware este debe contener objetivos de cómo restaurar los servicios de forma rápida, eficiente y con el menor tiempo, costos y perdidas posibles.

  El área de sistemas cuenta con personal altamente calificado, capaz de solucionar cualquier problema que se presente aun cuando el plan de contingencia no esté documentado, el área de sistemas ofrece solución casi inmediata a problemas relacionados con el hardware de comunicaciones, servidores y equipos de cómputo**.**

- En la sede EPS Emssanar zonal Ipiales existe ubicación inadecuada de los equipos de comunicación (modem, servidor, patch panel).

  Impacto. La ubicación inadecuada de los equipos de comunicación (switche, router, etc) así como los cables quedan expuestos completamente al polvo, humedad y caídas, por estar en el mismo espacio de las oficinas de atención al cliente provocando daños y/o pérdidas de equipos, las conexiones en los equipos o en el panel de empalme pueden ser manipuladas por cualquier

persona, el daño o pérdida de algún equipo activo genera pérdida de información o el cambio de equipos por consiguiente gastos para comprar o remplazar equipos.

Recomendación. En esta sede se recomienda que los equipos activos (switche, router, etc) se acojan a la norma ANSI/TIA/EIA-569-A, los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

- En Cresemillas, la seguridad del cuarto de comunicaciones o Rack no sigue las normas de seguridad establecidas en el estándar ANSI/TIA/EIA-569.

  Impacto. La falta de seguridad del cuarto de comunicaciones en la sede Cresemillas puede generar perdidas o robos, por ser un lugar muy grande que se presta para guardar objetos diferentes a equipos de comunicación y se ha tomado como bodega para guardar tubos y cosas de construcción, el techo es de eternit y tiene escapes de aire, lo que facilita la entrada de polvo a los equipos de comunicación, los cables sueltos hace que no cumpla con la norma ANSI/TIA/EIA-569, esto hace que la distribución del cableado no sea ordenada ocasionando daños e interrupciones o atenuación de la Red, generando mal funcionamiento de desempeño de la Red.

  Recomendación. Se recomienda definir un espacio adecuado para el lugar donde está instalado el cuarto de comunicaciones donde se ajuste a las normas de seguridad, se debe evitar el uso de cielos falsos por seguridad y para evitar la entrada de polvo a los equipos de comunicaciones, estos no deben compartir el espacio con otro elementos diferentes a las comunicaciones, el cuarto de comunicaciones es muy grande por eso es recomendable acondicionar parte del espacio teniendo en cuenta las medidas adecuadas y que se ajuste a la norma para proteger los recursos que forman parte de los equipos de comunicación, los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación.

- En la fundación Emssanar y en la IPS Lorenzo existen problemas de conectividad a Internet con baja velocidad, bloqueo y limitación de acceso a internet.

  Impacto: El hecho de que en la sede Fundación Emssanar y en la sede San Lorenzo haya internet con baja velocidad, bloqueo y limitación de acceso hace que se presenten dificultades para realizar diferentes proyectos que se adelantan dentro de estas sedes retrasando así las funciones que se deben realizar.

  Recomendación. Se recomienda dar acceso a internet bajo ciertas restricciones que no afecte el desarrollo y desempeño de estas sedes, también

es importante realizar un mantenimiento y revisión constante del la red de internet, para evitar o identificar fallas en el servicio.

Fortaleza. En las sedes se encontró debilidad de conectividad, sin embargo el área de sistemas esta en continuo control y evaluación del servicio de internet que provee a las sedes interconectadas, además el objetivo primordial del nivel de cobertura es interconectar todas las sedes y municipios del departamento de Nariño y así mismo ofrecer un buen servicio.

HARDWARE DE SERVIDORES

- En Emssanar ESS, el espacio donde se encuentran ubicados los servidores no cuenta con materiales incombustibles.

  Impacto. El no contar con materiales incombustibles puede causar daños irreversibles, un accidente provocado por el fuego causaría cese de actividades, pérdidas económicas y desastres catastróficos.

  Recomendación. Es importante que el espacio donde se encuentran ubicados los servidores, como paredes, suelo, techo, mesas, estanterías, cuente con pintura resistente al fuego, lavable, mate y de color claro, como también crear medidas de protección contra inundaciones y otros peligros físicos que afecten el lugar donde se encuentran los servidores.
- En Emssanar ESS, donde se encuentran ubicados los servidores no existen alarmas ni cámaras de seguridad.

  Impacto. El que no haya alarmas ni cámaras de seguridad, facilita robos o ataques contra los activos de la empresa, exponiendo así los recursos tecnológicos.

  Recomendación. Se recomienda la instalación de una cámara de seguridad o un sistema de alarma, necesarios en todas las empresas para reforzar la seguridad, estos sistemas ubicados en sitios estratégico, pueden detectar fácilmente la presencia de extraños lo cual evitaría que los equipos estén en riesgo o peor aun la perdida de información.

- En Emssanar ESS, en cuanto a las condiciones físicas el espacio donde se encuentran ubicados los servidores no es el adecuado.

  Impacto. El espacio donde se encuentran los servidores y equipos de comunicaciones al no contar con un buen ambiente físico (movilidad y espacio) en caso de presentarse una emergencia dificulta la evacuación del personal.

  Recomendación. Es importante que el espacio donde se encuentran ubicados los servidores cuente con un sitio apropiado de acuerdo a los

requerimientos de la norma EIA/TIA 569A.en cuanto a la altura mínima libre recomendada del cielo raso es de 2.6 metros, debe contar con un espacio adecuado donde se pueda circular fácilmente.

HARDWARE DE EQUIPOS DE CÓMPUTO

- En la Fundación Emssanar el espacio donde se encuentran ubicados los equipos de computo es limitado no se acoge a la norma EIA/TIA 569A.

  Impacto. En caso de presentarse una emergencia o desastres, la falta de un espacio apropiado para la ubicación de los equipos de computo, dificulta la evacuación del personal que allí labora donde cada empleado realiza una labor diferente, poniendo en riesgo la vida de estas personas.

  Recomendación. El espacio donde están ubicados los equipos de cómputo debe cumplir con la norma ANSI/TIA/EIA-569-A que brinde la posibilidad de movilidad de las personas ya que en algunas oficinas el espacio es limitado.

- En las sedes Fundación Emssanar y en Cresemillas en el Centro de Contactos existe deficiencia en cuanto al mantenimiento de los equipos de cómputo y actualizaciones de programas de antivirus.

  Impacto. La falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando en esta sede que los agentes de Contactos permanentemente tengan que estar cambiando de equipos, o peor aun cuando un equipo deja de funcionar generara más gastos.

  Recomendación. La falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando en esta sede que los agentes de Contactos permanentemente tengan que estar cambiando de equipos, o peor aun cuando un equipo deja de funcionar generara más gastos. Se recomienda realizar mantenimiento preventivo y correctivo de manera frecuente en estas sedes, visitarlas periódicamente para hacer una evaluación del comportamiento y funcionamiento del hardware, realizar actualizaciones de software que responda a las necesidades del trabajo a realizar, también es necesario concientizar al personal que maneja los equipos de cómputo en cuanto al cuidado y limpieza, dar a conocer con anterioridad el cronograma de mantenimiento al personal porque muchas veces las actividades se ven interrumpidas debido al mantenimiento.

- En Emssanar E.S.S, el área de soporte y mantenimiento el espacio donde se presta este servicio no es adecuado.

  Impacto. La falta de espacio del área de soporte y mantenimiento dificulta las actividades que allí se realizan, por ejemplo cuando se presentan situaciones

de reporte de varios equipos de las diferentes sedes el espacio es limitado generando estrés e incomodidad del personal que allí labora generando atrasos en la solución del reporte.

Recomendación. Se recomienda tomar medidas de acción que permitan provisionar el espacio de soporte y mantenimiento que asegure un servicio adecuado y oportuno.

ASEGURAMIENTO ELECTRICO

- En Emssanar ESS el diagrama de red eléctrica no está actualizado.

  Impacto. El no tener un diagrama de red eléctrica actualizado no solo hace que se ignoren cambios que se pudieron haber realizado, también puede ocasionar accidentes catastróficos pues impide ver donde puede estar fallando la red y realizar su mantenimiento respectivo.

  Recomendación. Se recomienda realizar las actualizaciones del diagrama de red eléctrica donde se identifiquen los cambios que se han realizado últimamente o si no se han realizado cambios que se deje observaciones de ello, un diagrama actualizado facilita realizar mantenimiento oportuno, permite vigilar variables de riesgo y elaborar informes de desempeño.

- En la Fundación Emssanar la red eléctrica no es segura por falta de UPS y reguladores.

  Impacto. La insuficiencia de reguladores hace que algunos equipos se conecten directamente a la energía, exponiendo a los equipos a picos altos y bajos de energía lo que podría generar daños irreversibles en gran parte del hardware, provocando gastos mayores. La falta de seguridad de la red eléctrica afecta también la seguridad de las personas y los equipos, provocando accidentes como incendios causados por sobrecarga eléctrica.

  Recomendación. Verificar que toda la instalación este a su vez conectada a tierra, debe existir un sistema de protección en caso de falla del fluido eléctrico como es el caso de UPS y puestas a tierra y reguladores. Utilizar sistemas de alimentación ininterrumpida, que permitan evitar una catástrofe y de esta manera corregir las deficiencias de la red eléctrica. Se recomienda que en la sede Fundación Emssanar la red eléctrica se acoja a la norma EAI/TIA 568.
- En la sede Laboratorio Clínico Emssanar no hay generadores de corriente si se fuese la energía.

  Impacto. Un apagón de energía por un largo periodo puede afectar el correcto funcionamiento de esta sede y generar un alto coste financiero, ya que se puede perder información, resultados de laboratorio, tiempo, etc.

Recomendación. En esta sede por la función que desempeña y los equipos que utiliza para prestar el servicio a usuarios, deben contar con la seguridad de que en dado caso en que llegase a irse la energía puedan contar con un suministro como generador de corriente ininterrumpida que les permita terminar dicha acción que se esté ejecutando y no cancelarse repentinamente.

- En la sede EPS Emssanar zonal Ipiales el tendido de cable no se acoge a la norma EIA/TIA-568 (Canaleta en el piso, cables sueltos, canaletas abiertas).

Impacto. La falta de seguridad de una red eléctrica con canaletas abiertas, cables sueltos y red eléctrica tendida en el piso, podría generar accidentes a quienes laboran en los puestos de trabajo, se corren riesgos significativos que pueden generar problemas intermitentes difíciles de diagnosticar, provocando deterioros importantes en los dispositivos de red incluso generando daños en los equipos de computo y comunicación.

Recomendación. En la sede EPS Emssanar zonal Ipiales se debe cumplir con los requerimientos mínimos del cableado estructurado y de telecomunicaciones, se recomienda hacer una instalación independiente regulada para la conexión de los equipos con base a la norma NTC2050, también que se acoja a la norma EIA/TIA 568. También se recomienda realizar de manera urgente el mantenimiento de la red eléctrica, que permita revisión de los cables salidos de las canaletas, en caso contrario adecuar las instalaciones existentes para cumplir con los requerimientos necesarios que garanticen la seguridad física y lógica de los recursos TI.

SEGURIDAD FISICA DEL HARDWARE DE COMUNICACIONES, SERVIDORES Y EQUIPOS DE CÓMPUTO.

- En las sedes SIAU, EPS Emssanar zonal Ipiales y en atención al usuario Emssanar Córdoba no hay extintor.

Impacto. El que no haya un extintor en una oficina, donde se sabe que se trabaja utilizando diferentes equipos conectados a energía hace que se presente en las sedes o en la empresa como tal factores de riesgo que inciden en el buen funcionamiento empresarial creando falencias bajas que se pueden convertir en graves si llegasen a ocurrir. El no hacerles el respectivo mantenimiento a los extintores causaría que estos estén en la empresa pero vencidos y quizá en caso de presentarse un incendio lo que genere sea un accidente fatal de la persona que lo manipule en ese momento.

Recomendación. Realizar una evaluación de todas las sedes en cuanto a seguridad de establecimientos o sedes en este caso con el fin de disponer del número total de extintores y dotar de estos a las sedes, igualmente realizar

mantenimiento de los mismos. Como también capacitar a todo el personal del centro de trabajo sobre los conocimientos básicos del fuego y en el manejo de los extintores.

- En las sedes Laboratorio Clínico Emssanar y en la IPS Lorenzo no hay seguridad de vigilancia.

  Impacto. La falta de un vigilante de seguridad hace más vulnerable el acceso a las instalaciones, poniendo en peligro la seguridad de los bienes de la empresa como también la del personal que labora en esa sede.

  Recomendación. En las sedes Laboratorio Clínico Emssanar y en IPS Lorenzo se debe establecer medidas de seguridad que permitan garantizar seguridad tanto del personal como de los recursos TI y se debe tener en cuenta lo siguiente: control de la entrada y salida de las instalaciones de estas sedes (Identificación de todo individuo que ingresa), realizar requisas a las personas que ingresan y salen de las instalaciones y registro de equipos de cómputo, portátiles que ingresan y que salen de las sedes.

INDICADORES DE FUNCIONAMIENTO

Fortalezas. En cuanto a indicadores de funcionamiento del área de sistemas, mediante la aplicación de técnicas y herramientas de auditoría se identifico el cumplimiento de los objetivos de cada indicador, además la evaluación de estos esta soportada bajo el **Software Estratega**, este es un sistema de apoyo que mide los indicadores, mide su avance y desempeño, encontrando fortalezas en:

Nivel de cobertura: de acuerdo al POA 2011 se cumple con el objetivo propuesto que es lograr la interconexión de las 142 sedes de Emssanar del departamento de Nariño y que hasta la fecha se han interconectado 141, número significativo para la empresa, por lo que se puede decir que el objetivo de este nivel en el POA propuesto se está cumpliendo satisfactoriamente.

Nivel Obsolescencia: se realiza a través de una serie de pasos para poder dar de baja a un equipo y se registra este en la base de datos ZONIFICACION CENTRAL, donde se verifica que los equipos registrados como obsoletos en esta base ya no estén en uso y de acuerdo a la evaluación realizada a este nivel lo anterior se cumple.

Nivel de soporte tecnológico: mide la optimización del soporte tecnológico, es decir evalúa toda solución de información, soporte e infraestructura técnica y tecnológica contemplados en los Planes de mantenimiento, planes de compras, proyecto seguridad, proyecto telefonía zonal, entre otros. Donde se

identifico que en el proceso continuamente se evalúa los avances de los objetivos de cada plan propuesto.

Nivel tiempo fuera de servicio: Numero de horas fuera de servicio (servidores, servicios esenciales y canal). El objetivo de este indicador es que a través del control y mantenimiento continuo se mejore la prestación de servicio de interconexión y así reducir al máximo el tiempo fuera de servicio. Según estadística realizada anualmente se identifica que el objetivo propuesto se cumple.

PLAN DE MEJORAMIENTO

Con la realización de la auditoria se espera que esta genere un plan estratégico que asegure el manejo y control de la documentación concerniente al hardware de las comunicaciones, servidores, equipos de cómputo e indicadores de funcionamiento a fin de asegurar la calidad en el área de sistemas de la empresa Emssanar E.S.S y que mediante las vulnerabilidades encontradas esta entidad diseñe un plan de mejoramiento que permita mitigar los riesgos y asegurar los procesos del área de sistemas en cuanto a:

- Gestión de riesgos de hardware de comunicaciones.
- Documentar la gestión de la red de comunicaciones
- Aseguramiento físico y eléctrico de los equipos de cómputo, los servidores y las comunicaciones.
- Mantenimiento de equipos de cómputo, servidores, equipos de comunicación y red eléctrica.
- Seguridad física de las instalaciones.
- Documentación de planos de red.

Entre otras recomendaciones descritas al final del documento.

Atentamente,

LAURA YANETH NOGUERA QUENGUAN
EDY YANIRA SANCHEZ PERENGUEZ
Auditores

3. MANUAL DE USUARIO

Para el hallazgo del Dominio: **Dar soporte y servicio (DS),** en el proceso administración de ambiente físico (DS12) tenemos el siguiente ejemplo:

Emssanar E.S.S. ¡Siempre cerca de Usted!	**HALLAZGOS**	**REF** PLAN DS12_3_7

ENTIDAD AUDITADA	Empresa Solidaria De Salud EMSSANAR E.S.S – Nariño			**PAGINA**	**1 DE 3**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Riesgos del hardware de servidores, comunicaciones y equipos de cómputo.		
RESPONSABLES	Laura Yaneth Noguera Q y Edy Yanira Sánchez P.				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Dar Soporte y Servicio (DS)	**PROCESO**	Administración de Ambiente Físico (DS12).		

HALLAZGO	En Emssanar ESS, no existen sistemas de alarmas, ni cámaras de seguridad, ni detección de movimiento, en la sede Fundación Emssanar no hay señales de evacuación, en las sedes Laboratorio Clínico y en IPS Lorenzo no hay seguridad de vigilancia.

RECOMENDACIONES

La seguridad en un cuarto de comunicaciones es primordial debido a los riesgos que se pueden presentar como robos o atentados contra los recursos de TI; cámaras de seguridad es uno de los aparatos más populares que se puede utilizar, una cámara no puede parar a nadie de robar, pero si ofrece tranquilidad y seguridad, lo mismo que un sistema de alarma, colocado en un sitio estratégico, puede detectar fácilmente la presencia de extraños lo cual evitaría que los equipos estén en riesgo o peor aun la perdida de información.

- Las instalaciones de la Fundación Emssanar dentro de los objetivos deberá proporcionar unas orientaciones básicas para facilitar el proceso de la señalización relativa a las situaciones y actuaciones de emergencia, esto con el fin de garantizar la seguridad y salud de los trabajadores. Esta señalización abarcara tanto la señalización de la localización de los medios de protección contra incendios como la señalización de evacuación, salvamento y socorro en sus diferentes tipos y modalidades.
- La sede IPS Lorenzo por ser una de las sedes que prestan atención al usuario y como tal atiende un gran número de usuarios se debe implementar medidas de seguridad para el acceso a la entidad, debe existir una persona encargada de la seguridad de la sede.
- En las sedes Laboratorio Clínico Emssanar y en IPS Lorenzo se debe establecer medidas de seguridad que permitan garantizar seguridad tanto del personal como de los recursos TI de la sede.

IMPACTO	El que no haya cámaras de seguridad, alarmas, ni detectores de movimiento, impide evitar robos o ataques contra los activos de la empresa. El que no haya señalización de evacuación en caso de presentarse una emergencia genera diferentes tipos de problemas a la cual la empresa queda expuesta por hacer caso omiso a esta recomendación. En caso de presentarse, la sede queda expuesta a una investigación exhaustiva permitiendo identificar situaciones de riesgo desconocidas o poco favorables o quizá innecesarias. Un vigilante de seguridad es la persona encargada de proteger la integridad física de las personas y los bienes materiales de la empresa donde labora, razón por la cual si no lo hay en un de estas sedes, se presenta inseguridad tanto del personal como de los bienes que en ella existen, causando inestabilidad laboral y material, en este caso en Laboratorio y en IPS Lorenzo. El ingreso de personas mal intencionadas genera inestabilidad e inseguridad a los usuarios (pacientes).

PROBABILIDAD – IMPACTO			
Probabilidad	Medio	**Impacto**	Alto

EVIDENCIAS	ANEXO 41_ENT DS12_SP_1 ANEXO 26_DS12_FE ANEXO 25_DS12_LAB ANEXO 29_DS12_LZ

AUDITORES RESPONSABLES
EDY YANIRA SANCHEZ P.
LAURA YANETH NOGUERA Q.

En el formato definido para sustentar los Hallazgos se encuentra el campo **Evidencias,** que son las pruebas que pueden ser entrevistas o cuestionarios que sustentan la veracidad de este hallazgo.

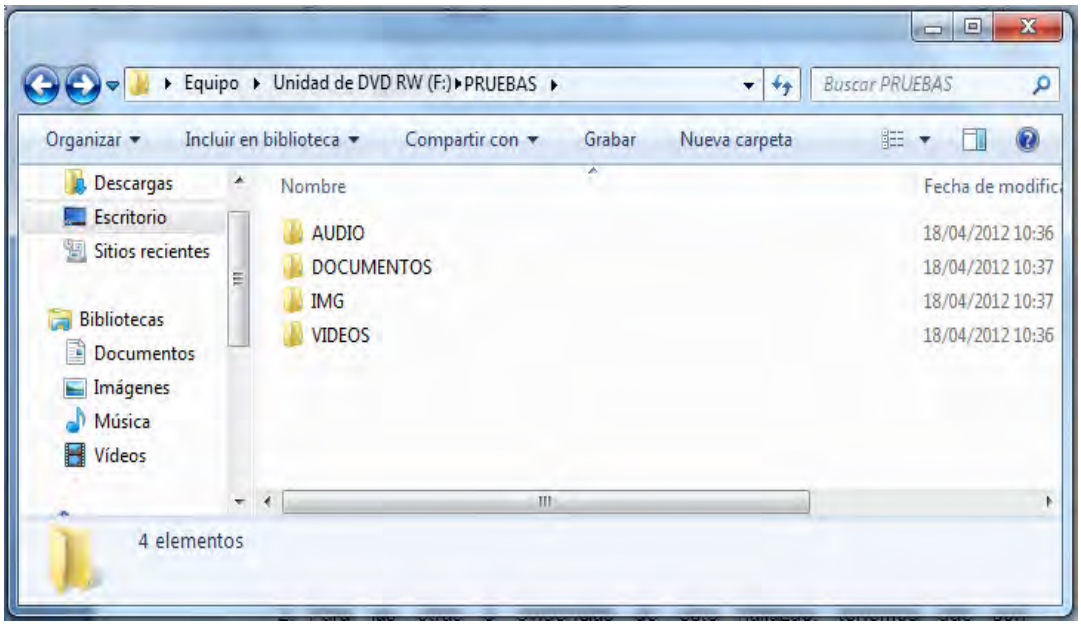
Es importante mencionar que los nombres de las evidencias tanto en:

- Entrevistas ejm: ANEXO 41_ENT DS12_SP_1, las dos penúltimas letras significan el nombre de la sede en la cual se encontró el hallazgo, en este caso el hallazgo pertenece a la Sede Principal de Pasto y el numero seguido indica la cantidad de entrevistas del dominio que en este caso es al DS12 realizadas en esta sede.

- Cuestionarios ejm: ANEXO 26_DS12_FE, donde las dos últimas letras hacen referencia a que el hallazgo fue encontrado en la sede Fundación Emssanar.

Cabe aclarar que en el CD se encuentran dos carpetas ANEXOS y PRUEBAS, al entrar a la carpeta PRUEBAS se encuentra los siguiente (Figura 18).

Figura 18: Listado de Carpetas (PRUEBAS)



Donde se encuentran todas las pruebas que verifica toda la información recolectada en el proceso de la auditoria.

Para poder acceder a estas pruebas se debe seguir los siguientes pasos definidos así:

1. En el hallazgo **PLAN DS12_3_7** tomado como ejemplo tenemos cuatro evidencias donde una es entrevista, por lo que esta referenciada como: **ANEXO 41_ENT DS12_SP_1**, así entonces para llegar a los documentos de prueba se debe:

   - Ir a la carpeta ANEXOS
   - Dentro de la carpeta Anexos entrar a la carpeta de ENTREVISTAS **(ANEXOS\ENTREVISTAS\ANEXO 41_ENT DS12_SP_1)**, donde están numerados todas las entrevistas aplicadas en la auditoria, cabe aclarar que estas entrevistas residen también en el archivo corriente en físico firmadas por las personas entrevistadas como prueba veraz de todos los hallazgos encontrados.

2. Las siguientes 3 evidencias de este hallazgo son cuestionarios, donde se toma

como ejemplo: **ANEXO 25_DS12_LAB**, donde nos vamos a encontrar con diferentes tipos de pruebas que pueden ser videos, audio y/o fotografías o entrevistas en físico como lo muestra la figura 18, para llegar a esta información se debe:

- Ir a la carpeta ANEXOS
- Dentro de la carpeta Anexos entrar a la carpeta de CUESTIONARIOS **(ANEXOS\CUESTIONARIOS\ ANEXO25)**, donde están numerados todos los cuestionarios aplicados en la auditoria.
- Para el **ANEXO25**, en el campo llamado fuente se registran los nombres de las evidencias que prueban la respuesta de los Sí o No y si estos existen, para este caso encontramos como prueba una entrevista en audio con su respectiva ruta de ubicación así **AUDIO\PR29_Aux At Usu_Laboratorio.**
- Si tomamos la evidencia **ANEXO 29_DS12_LZ**, lo mismo que el paso anterior, entramos a **ANEXOS\CUESTIONARIOS** y allí está el **ANEXO 29,** en el cual nos vamos a encontrar también con pruebas como fotografías, que para llegar a ellas seguimos la ruta de acceso **PRUEBAS\IMG\IMG_DS12_0021**.

3. Cabe aclarar que en alguno de los cuestionarios también se encuentran pruebas de video o documentos, para tener acceso a ellos simplemente se accede a la ruta **PRUEBAS\VIDEOS o PRUEBAS\DOCUMENTOS,** por ejemplo: **DOCUMENTOS\PR2_Instructivo de asignación de equipos**, que significa Prueba dos llamada Instructivo de asignación de equipos, así con los demás documentos existentes en la carpeta **DOCUMENTOS**, evidencia de que existen todos los documentos solicitados para la realización de la auditoria y que en los cuestionarios son requeridos como fuente.

4. CONCLUSIONES

- ✓ Actualmente la tecnología es una de las herramientas más importantes y más utilizadas por el hombre, a diario las empresas incorporan tecnología de punta en sus instalaciones con el fin de mejorar los procesos, razón por la cual es esencial velar por la seguridad y bienestar de los recursos tecnológicos que hacen parte del desarrollo y desempeño laboral y empresarial, para ello toda empresa pública o privada deben de someterse a un control estricto de evaluación de eficiencia y eficacia con el objetivo de que los diferentes procesos funcionen correctamente.

- ✓ Mediante el proceso de auditoría realizado en Emssanar ESS se logro determinar situaciones de debilidades en cuanto a la gestión de riesgos y seguridad física del hardware de las comunicaciones, servidores y equipos de cómputo, como también se identifico fortalezas en procesos de adquisición de infraestructura e indicadores de funcionamiento.

- ✓ Durante el desarrollo de la auditoría es importante mencionar que dentro del análisis y observación se percato que en Emssanar ESS no existen políticas para el análisis y la gestión de riesgos que permitan la identificación y clasificación de estos, por lo que impide determinar la probabilidad de ocurrencia e impacto, determinar controles de mitigación y la toma de decisiones frente a estos riesgos, teniendo en cuenta que estas políticas deben ser implantadas y que por medio de controles se prevenga la ocurrencia de situaciones de riesgo para la empresa y así asegurar la integridad en los todos los procesos.

- ✓ También, en Emssanar ESS hace falta realizar una revisión detallada de la red eléctrica, pues en muchas sedes se manifestó que hay inseguridad en la red eléctrica y se verifico mediante revisión visual, esta situación está afectando la seguridad de las personas y de los equipos pues se pueden provocar graves accidentes como incendios causados por sobrecarga eléctrica o descuido de cables sueltos o tendidos por el piso.

- ✓ La realización de la auditoría aporta considerables beneficios al área de sistemas de Emssanar E.S.S, los principales son mayor eficiencia en los procesos pertenecientes a esta área, desarrollar un plan de mejoramiento que permita garantizar la seguridad, confiabilidad y disponibilidad de los recursos tecnológicos, mediante los resultados obtenidos de la auditoria, entre otros.

- ✓ Y principalmente con la realización de la Auditoria Informática hace que como estudiantes y profesionales se hayan aplicado conocimientos y a la vez ampliado lo aprendido en las aulas de clases. Es importante la formación que se obtuvo en la Universidad ya que se cuenta con el conocimiento y capacidad para analizar diferentes situaciones a los que se expone la información identificando debilidades y fortalezas de los diferentes procesos que existen en una empresa, obteniendo como resultados generales mejorar la calidad de la información.

5. RECOMENDACIONES

- ✓ Realizar diferentes auditorias con el fin de evaluar todos los procesos que se desarrolla dentro de Emssanar E.S.S con el fin de mejorar en todos los campos y así ser una empresa que brinde en su totalidad un mejor servicio bajo los parámetro de calidad establecidos.

- ✓ Realizar la verificación de la información obtenida durante el proceso de la auditoría realizada, esto mediante herramientas de recolección de información como encuestas, entrevistas, cuestionarios, etc., realizados en Emssanar ESS.

- ✓ Visitar periódicamente las sedes o establecer medidas que permitan hacer una evaluación continua de las necesidades que se presenten en ellas, con el fin de solventar fallas en los diferentes procesos o actividades de los usuarios, así mismo cuando se reciba reportes de fallas de parte de las sedes establecer un periodo de tiempo para dar solución, esto con el fin de no alargar mucho tiempo en resolver el problema.

- ✓ Realizar planes de contingencia que permitan garantizar la continuidad de los servicios que garantice la conectividad de internet, mantenimiento y soporte técnico en todas las sedes, que son claves para el correcto funcionamiento de los procesos que se realizan en Emssanar ESS.

- ✓ Mantener el inventario de los equipos de cómputo, servidores, entre otros con todos los datos, acoplándose a como son llevadas las hojas de vida de los equipos con el fin de llevar un control y un registro adecuado de los activos de la empresa.

- ✓ Mantener actualizado el inventario de equipos de computo, ya que en la toma de datos en las diferentes visitas hechas a la sede principal como a las demás sedes se realizo un muestreo de las especificaciones técnicas de los equipos, donde se encontraron algunas inconsistencias en cuanto a algunos datos que no coinciden con las especificaciones técnicas de los equipos registrados en el inventario.

- ✓ Entregar al responsable de cada sede una copia del cronograma de actividades de mantenimiento con el fin de dar a conocer al personal de cada sede las fechas de mantenimiento con anterioridad para no afectar las actividades que se estén realizando en el momento de hacer el mantenimiento.

- ✓ Realizar actualización periódica del software y hardware garantizando así que los equipos estén en la capacidad de realizar actividades acordes al a las necesidades de cada usuario.

- ✓ Realizar planes de mejoramiento que ayuden a mejorar los procesos con el fin de mitigar los riesgos encontrados mediante el establecimiento de medidas preventivas y correctivas que permitan tener definido medidas a tomar en caso de presentarse en la empresa.

BIBLIOGRAFIA

Arens, Alvin A. Auditoria un Enfoque Integral. 6 Edición. México: Prentice Hall, 1996.

Echenique García, José Antonio. Auditoría en Informática. 2 Edición. México: Mc Graw Hill, 2001.

GUSTIN Enith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

TESIS

BURGOS, Jenny. DOMINGUEZ, Carolina. Auditoria al Módulo de Historia Clínica Electrónica del Sistema de Información del Hospital Universitario Departamental de Nariño. Universidad de Nariño. 2007.

CAICEDO, Liliana. ORDOÑEZ, Claudia. Técnicas de Auditoria de Sistemas Aplicadas al Proceso de Contratación y Páginas Web en Entidades Oficiales del Departamento de Nariño. Universidad de Nariño. 2010.

ESTRADA, Oscar. Auditoría de Sistemas Aplicada al Sistema Integral de Información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto. Universidad de Nariño. 2007

BIBLIOWEB

http://benmp82.galeon.com/funsis.htm (Consultado, Julio 2011)

http://www.monografias.com/trabajos14/auditoria/auditoria.shtml (Consultado, Julio 2011)

http://www.hondutel.hn/portal_transparencia/pdf/auditoriainterna-2.pdf (Consultado, Julio 2011)

http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml (Consultado, Agosto 2011)

http://www.gerencie.com/auditoria-financiera.html (Consultado, Agosto 2011)

http://www.definicion.org/auditoria-operacional (Consultado, Agosto 2011)

http://members.tripod.com/~Guillermo_Cuellar_M/integral.html (Consultado, Agosto 2011)

http://www.mitecnologico.com/Main/ConceptosAuditoriaYAuditoriaInformatica (Consultado, Agosto 2011)

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml (Consultado, Agosto 2011)

http://www.monografias.com/trabajos5/audi/audi.shtml (Consultado, Agosto 2011)

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml (Consultado, Septiembre 2011)

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm#p2-1-1 (Consultado, Septiembre 2011)

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml (Consultado, Septiembre 2011)

www.adacsi.org.ar/files/es/content/146/Standards.doc (Consultado, Septiembre 2011)

http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf (Consultado, Marzo del 2011)

http://www.channelplanet.com/index.php?idcategoria=13932 (Consultado, Noviembre 2011)

http://html.rincondelvago.com/dfd.html (Consultado, Noviembre 2011)

http://www.emssanar.org.co/contenidos/COOEmssanarIPS/rendicion_de_cuentas/CODIGO_DE_BUEN_GOBIERNO_Y_ETICA.pdf (Consultado, Junio 2011).

http://www.articulo.org/articulo/9219/definicion_de_eps.html (Consultado, Noviembre 2011).

http://www.articulo.org/1/admin (Consultado, Noviembre 2011).

ANEXOS

CUADROS DE DEFINICIÓN_PLANEACION Y ORGANIZACION

ANEXO 1. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO3. Determinar la Dirección Tecnológica - PLAN PO3-1.

ANEXO 2. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO4. Definición de la organización y las relaciones de TI - PLAN PO4-1.

ANEXO 3. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO9. Evaluación de riesgos - PLAN PO9-1.

CUADROS DE DEFINICIÓN_ADQUISICION E IMPLEMENTACION

ANEXO 4. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI3. Adquisición y Mantenimiento de la Infraestructura Tecnológica - PLAN AI3-1.

ANEXO 5. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI5. Adquirir recursos TI - PLAN AI5-1.

ANEXO 6. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI6. Administrar Cambios - PLAN AI6-1.

CUADROS DE DEFINICIÓN_ENTREGA DE SERVICIOS Y SOPORTE

ANEXO 7. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS4. Garantizar la continuidad del servicio - PLAN DS4-1.

ANEXO 8. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS8. Administrar la mesa de servicios y los incidentes - PLAN DS8-1.

ANEXO 9. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS12. Administración de Instalaciones - PLAN DS12-1

CUADROS DE DEFINICIÓN_MONITOREAR Y EVALUAR

ANEXO 10. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - ME1. Monitorear y evaluar el desempeño de TI - PLAN ME1-1

ANEXO 11. Cuadro de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - ME2. Monitorear y evaluar el control interno - PLAN ME2-1

CUESTIONARIO CUALITATIVO_PLANEACION Y ORGANIZACIÓN

ANEXO 12. Cuestionario Cuantitativo - PO3. Determinar la Dirección Tecnológica -PLAN PO3_2_SP.

ANEXO 13. Cuestionario Cuantitativo - PO4. Definición de la organización y las relaciones de TI PLAN PO4_2_SP

ANEXO 14. Cuestionario Cuantitativo - PO9. Evaluación de riesgos - PLAN PO9_SP

CUESTIONARIO CUALITATIVO_ADQUISICION E IMPLEMENTACION

ANEXO 15. Cuestionario Cuantitativo - AI3. Adquirir y Mantener Infraestructura Tecnológica - PLAN AI3_2_SP

ANEXO 16. Cuestionario Cuantitativo - AI5. Adquirir recursos TI - PLAN AI5_2_SP.

ANEXO 17. Cuestionario Cuantitativo - AI6. Administrar Cambios - PLAN AI6_2_SP

CUESTIONARIO CUALITATIVO_ENTREGA DE SERVICIOS Y SOPORTE

ANEXO 18. Cuestionario Cuantitativo - DS4. Garantizar la continuidad del servicio - PLAN DS4_2_SP

ANEXO 19. Cuestionario Cuantitativo - DS8. Administrar la mesa de servicios y los incidentes - PLAN DS8_2_SP

ANEXO 20. Cuestionario Cuantitativo - DS8. Administrar la mesa de servicios y los incidentes - PLAN DS8_2_E.IPS

ANEXO 21. Cuestionario Cuantitativo - DS8. Administrar la mesa de servicios y los incidentes - PLAN DS8_2_LAB

ANEXO 22. Cuestionario Cuantitativo - DS8. Administrar la mesa de servicios y los incidentes - PLAN DS8_2_LZ

ANEXO 23. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_SP

ANEXO 24. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_E.IPS

ANEXO 25. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_LAB

ANEXO 26. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_FE

ANEXO 27. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_SIAU

ANEXO 28. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_CC

ANEXO 29. Cuestionario Cuantitativo - DS12. Administración del Ambiente Físico - PLAN DS12_2_LZ

CUESTIONARIO CUALITATIVO_MONITOREAR Y EVALUAR

ANEXO 30. Cuestionario Cuantitativo - ME1. Monitorear y Evaluar Desempeño de TI – PLAN ME1_2_SP

ANEXO 31. Cuestionario Cuantitativo - ME2. Monitorear y Evaluar el Control Interno - PLAN ME2_2_SP

ENTREVISTAS_PLANEACION Y ORGANIZACIÓN

ANEXO 32. Entrevista - PO3. Determinar la Dirección Tecnológica - ENT PO3_SP.

ANEXO 33. Entrevista - PO9. Evaluación de riesgos - ENT PO9_SP

ANEXO 34. Entrevista - PO9. Evaluación de riesgos - ENT PO9_FE

ANEXO 35. Entrevista - PO9. Evaluación de riesgos - ENT PO9_CC

ANEXO 36. Entrevista - PO9. Evaluación de riesgos - ENT PO9_LZ

ENTREVISTAS_ ADQUISICION E IMPLEMENTACION

ANEXO 37. Entrevista - AI3. Adquirir y Mantener Infraestructura Tecnológica- ENT AI3_SP_1

ANEXO 38. Entrevista - AI3. Adquirir y Mantener Infraestructura Tecnológica- ENT AI3_SP_2

ANEXO 39. Entrevista - AI5. Adquirir recursos TI - ENT AI5_SP_1

ENTREVISTAS_ ENTREGA DE SERVICIOS Y SOPORTE

ANEXO 40. Entrevista - DS8. Administrar la mesa de servicios y los incidentes - ENT DS8_E.IPS

ANEXO 41. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_SP_1

ANEXO 42. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_SP_2

ANEXO 43. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_E.IPS

ANEXO 44. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_LAB

ANEXO 45. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_FE

ANEXO 46. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_CC

ANEXO 47. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_SIAU

ANEXO 48. Entrevista - DS12. Administración del Ambiente Físico - ENT DS12_LZ

ENTREVISTAS_ MONITOREAR Y EVALUAR

ANEXO 49. Entrevista - ME1. Monitorear y Evaluar Desempeño de TI - ENT ME1_SP