# AUDITORÍA DE SISTEMAS APLICADA A LOS MÓDULOS DE FACTURACIÓN, CONSULTAS E HISTORIA CLÍNICA DEL SOFTWARE INFO-SALUD EN LA IPS INDÍGENA GUAITARA DEL MUNICIPIO DE IPIALES.

**MELANNY CATHERINE OVIEDO MESÍAS**
**OSCAR MAURICIO AZA ARÉVALO**

**UNIVERSIDAD DE NARIÑO**
**FACULTAD DE INGENIERÍA**
**PROGRAMA DE INGENIERÍA DE SISTEMAS**
**SAN JUAN DE PASTO**
**2015**

# AUDITORÍA DE SISTEMAS APLICADA A LOS MÓDULOS DE FACTURACIÓN, CONSULTAS E HISTORIA CLÍNICA DEL SOFTWARE INFO-SALUD EN LA IPS INDÍGENA GUAITARA DEL MUNICIPIO DE IPIALES.

**MELANNY CATHERINE OVIEDO MESÍAS**
**OSCAR MAURICIO AZA ARÉVALO**

**Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas**

**DIRECTORES**
**ING. FRANCISCO NICOLÁS SOLARTE SOLARTE**
**ING. JOSÉ JAVIER VILLALBA ROMERO**

**UNIVERSIDAD DE NARIÑO**
**FACULTAD DE INGENIERÍA**
**PROGRAMA DE INGENIERÍA DE SISTEMAS**
**SAN JUAN DE PASTO**
**2015**

## NOTA DE RESPONSABILIDAD

”Las ideas y las conclusiones aportadas en el presente trabajo son responsabilidad exclusiva de sus autores”

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

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

San Juan de Pasto, Octubre de 2015

## AGRADECIMIENTOS

A Dios, por siempre estar ahí en todo el camino recorrido y su fortaleza para llegar hasta el final y alcanzar nuestro objetivo.

A nuestras familias, por su apoyo, comprensión y amor.

Al ingeniero Francisco Nicolás Solarte, por su colaboración y tiempo dedicado en el desarrollo del trabajo.

Al Ingeniero German Darío Burbano, por su apoyo, paciencia y colaboración incondicional a lo largo del desarrollo de este trabajo.

A la IPS Indígena Guaitara de Ipiales y su representante legal, la Doctora Olga Potosí, por la colaboración prestada para la ejecución y culminación de este trabajo.

A nuestros profesores, por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional.

A nuestros amigos y compañeros, con quienes vivimos tantos momentos durante nuestra trayectoria en la Universidad hasta este punto, apoyándonos mutuamente en nuestra formación profesional.

A todas aquellas personas que contribuyeron en la realización de este trabajo.

## DEDICATORIA

A mi madre, Ayda Mesías Escobar, por la educación recibida, por corregir mis errores, por los sabios consejos que siempre me ha brindado, por cultivar e inculcar ese gran don de la responsabilidad, por su amor y apoyo incondicional.

A mi padre, Álvaro Oviedo, por todo el cariño y compresión brindado en el transcurso de mi vida y de mi carrera profesional.

A mis hermanos que siempre han estado junto a mí, que han tenido el mismo sentir en mis logros y dificultades y que con su amor me alentaron a seguir luchando por mis metas.

A mi compañero de trabajo y amigo Oscar Mauricio Aza, con quien compartí maravillosas y significativas experiencias y de quien he recibido las mayores lecciones de amistad, compañerismo y solidaridad.

A mis docentes, por su esfuerzo y dedicación al brindarme lo mejor de sus enseñanzas.

A mis amigos y compañeros que me apoyaron sin importar la situación, a ellos gracias porque valoran lo que soy, por eso los llevo en mi corazón.

Melanny Catherine Oviedo Mesías

## DEDICATORIA

A mis Padres, por sus enseñanzas, por su ejemplo, cariño y valores inculcados que hicieron que todo esto fuera posible.

A mi hermano por su amistad, colaboración y apoyo incondicional que me hace saber que siempre estará ahí cuando lo necesite.

A mi amiga, Melanny Oviedo, por su amistad y paciencia en cada una de las etapas que he tenido el gusto de compartir con ella.

A mis amigos, por su comprensión en los momentos de dificultad que enseñan que todo tiene solución.

Oscar Mauricio Aza Arévalo

## RESUMEN

La búsqueda de acceso, calidad y eficiencia en la prestación de servicios conforme a lo planteado por el Ministerio de Salud y Protección Social lleva a aplicar controles y evaluación a todas y cada una de las áreas que conforman la entidad, en este sentido el software de administración y gestión INFO-SALUD no se le ha realizado un análisis previo que permita establecer el grado de confiabilidad en los procedimientos que se ejecutan en los módulos de facturación, inventarios, historia clínica (medicina general, odontología, laboratorio) que apoyan las áreas más importantes para la ejecución de la IPS Indígena Guaitara del municipio de Ipiales.

Esta auditoría de sistemas parte de la necesidad de evaluar las oportunidades de mejoramiento y fortalezas del software que administra la información de esta entidad, teniendo en cuenta la importancia del mismo dentro de la institución puesto que gracias a este software, se tiene un control general de la entidad y sus funciones. El fin principal de aplicar una auditoría es ayudar a presentar las respectivas recomendaciones que apoyarán a los planes de mejoramiento a realizarse en esta entidad.

La auditoría de sistemas aplicada al software INFO-SALUD es de gran importancia ya que permitirá analizar y evaluar los procesos que se llevan a cabo en las diferentes áreas que conforman a la IPS Indígena Guaitara del municipio de Ipiales.

Para el desarrollo de este trabajo se tomó como guía el estándar COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) el cual proporcionó un marco de trabajo (framework) para el análisis de los niveles de seguridad y control necesarios para proteger la información que es el activo más importante para la organización.

El trabajo contempla el proceso de auditoría a los módulos que posiblemente son los más afectados por la entrada de datos y salidas que produce el sistema para los usuarios, las funcionalidades existentes en cada uno de los módulos y la conexión con otros módulos que garantice la continuidad, disponibilidad, integridad y trazabilidad de los datos que circulan por el sistema.

## ABSTRACT

The search for access, quality and efficiency in the delivery of services as proposed by the Ministry of Health and Social Protection carries implement controls and evaluation of each and every one of the areas that make up the entity, however management software INFO-HEALTH has not made a prior analysis to establish the degree of reliability of the procedures runed in the modules for billing, inventory, medical history (general medicine, dentistry, laboratory) that support the most important areas for IPS Indigenous Guaitara of the Ipiales city.

This auditing-systems stems from the need to verify improvement opportunities and strengths of the software that manages information of this entity, needs to account for the importance within the institution because thanks to this we have a general control of the entity and its functions. The main purpose of implementing an audit is help to present their respective recommendations that will support the improvement plans to be held in this entity.

The auditing-systems applied to software INFO-SALUD is of great importance as it will analyze and evaluate the processes carried out in different areas that make up the IPS Indigenous Guaitara of the Ipiales city.

For the development of this project we used the standard COBIT (Control Objectives for Information and related Technology) which provides a framework (framework) for the analysis of the levels of security and control necessary to protect information it will be a guide the most important asset for the organization.

The project includes the audit process modules that are possibly the most affected by the input and outputs produced by the system for users, existing in each of the modules functionalities and connection with other modules to ensure continuity availability, integrity and traceability of the data circulating on the system.

**TABLA DE CONTENIDO**

**Pág.**

## LISTA DE CUADROS

**Pág.**

## LISTA DE FIGURAS

**Pág.**

## LISTA DE ANEXOS

**Pág.**

## GLOSARIO

**Administración:** conjunto de técnicas por medio de las cuales se determinan, clasifican y realizan los propósitos y objetivos de un grupo humano particular.

**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.

**Anamnesis:** parte de la historia clínica correspondiente al interrogatorio.

**Análisis de riesgo:** según [iso/iec guía 73:2002]: uso sistemático de la información para identificar fuentes y estimar el riesgo.

**Atención médica:** conjunto de actividades armónicamente integradas, realizadas en servicios de salud de distinto nivel de complejidad o en el seno de la comunidad y que tienen como objetivo, actuando sobre las personas, promover, proteger, recuperar y rehabilitar la salud física y mental de los individuos, incluyendo l atención de los mismos para su reubicación.

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

**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 de una organización.

**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 pérdida de los originales.

**Bases de datos:** colección de datos organizada de tal modo que el computador pueda acceder rápidamente a ella.

**Beneficiario:** persona que recibe los servicios de atención médica.

**Bitácora:** un cuaderno o publicación que permite llevar un registro escrito de diversas acciones. Su organización es cronológica, lo que facilita la revisión de los contenidos anotados.

**Capacidad de respuesta:** la capacidad de respuesta de un sistema cualquiera es su probabilidad media de producir, frente a una demanda, una respuesta de calidad aceptable, dentro de un margen de tiempo aceptable y a un costo aceptable.

**Calidad de los recursos:** características que deben presentar para satisfacción del usuario externo o interno.

**Centro de informática:** es un área de trabajo cuya función es la de concentrar, almacenar y procesar datos y funciones operativas de una entidad de manera sistematizada.

**COBIT:** *(control objetives for information and related technology),* objetivos de control para la información y tecnología relacionada; 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 entidades y auditores.

**Confiabilidad**: es el grado de estabilidad que presenta un instrumento al obtener el mismo resultado en oportunidades repetidas bajo condiciones idénticas.

**Continuidad:** capacidad del servicio de realizar actividades debidas en la secuencia apropiada y sin interrupción del proceso de atención al beneficiario, desde la primera atención hasta la satisfacción de sus necesidades, solicitudes y expectativas de salud.

**Contraseña:** se refiere al conjunto de caracteres ocultos que le permiten el acceso a un operario a utilizar cierta proporción de un sistema o a una red.

**Datos:** término general para la información procesada por un computador.

**Disponibilidad:** cantidad de recursos por unidad de población a atender. Si solo es una lista de recursos, se le denomina inventario.

**Efectividad**: conseguir mejoras en la salud mejorando el impacto de la morbilidad sobre una población definida. Consiste en la medición del grado en que una forma eficaz de intervención puede aplicarse o ponerse a disposición de todos los miembros de un grupo definido que podría resultar beneficiado.

**Eficacia**: capacidad de la ciencia y la tecnología para lograr un resultado favorable en casos individuales, con independencia de los recursos o insumos necesarios. Consiste en determinar objetivamente que una forma de intervención, preventiva, diagnóstica, curativa o restaurativa; es más útil y beneficiosa que inútil o perjudicial para alcanzar la finalidad preconizada, o que es más eficaz que el tipo de intervención que reemplazará, o que en realidad es mejor que no hacer nada.

**Eficiencia**: consiste en la medición del grado en que se puede alcanzar un nivel determinado de efectividad con un costo mínimo de personal, de recursos y fondos. Es la relación costo/ beneficio por la que se obtiene la mejor calidad al menor costo posible. Expresa los resultados finales obtenidos en relación con los costos en términos de dinero, recursos y tiempo

**Epicrisis:** conjunto de fenómenos que se presentan después de haber pasado la crisis de una enfermedad

**EPS:** entidad promotora de salud y es la encargada de promover la afiliación al sistema de seguridad social. Aquí no hay servicio médico, solo administrativo y comercial.

**Las evidencias:** son pruebas que sustentan la veracidad de un hallazgo.

**Hardware:** conjunto de componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador.

**Impacto:** es el resultado de una causa a largo plazo

**Información:** está constituida por un grupo de datos organizados, procesados y supervisados; la información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

**Infraestructura tecnológica:** es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que una empresa necesita tener en funcionamiento para poder llevar a cabo todas sus actividades.

**Instituto departamental de salud de Nariño:** establecimiento público descentralizado del orden departamental, dotado de personería jurídica, patrimonio propio y autonomía administrativa, con una junta directiva, un director nombrado por el gobernador del departamento y una planta de personal; sujeto a lo regulado en la ley 10 de 1990 y a las demás disposiciones que le son aplicables como establecimiento público.

**Inventario de activos:** lista de todos aquellos recursos (físicos de información, software, documentos, servicios), que tengan un valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.

**IPS**: instituciones prestadoras de servicios. Es decir, todos los centros, clínicas y hospitales donde se prestan los servicios médicos, bien sea de urgencia o de consulta.

**IPSI:** institución prestadora de salud indígena.

**Isaca:** *(information systems audit and control association),* es una asociación de auditoría y control de sistemas de información que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

**Kardex:** es un registro de manera organizada de la mercancía que se tiene en un almacén (entidad). Para hacerlo, es necesario hacer un inventario de todo el contenido, la cantidad, un valor de medida y el precio unitario.

**Misión**: declaración respecto al compromiso con los objetivos principales de una organización, discutidos y aceptados previamente por todos sus participantes. Por lo general, se espera que todo y cualquier miembro de la organización, desde el nivel elemental hasta el ejecutivo principal, pueda expresar con sus palabras la misión, la visión y los valores de la misma.

**Módulos:** hace referencia a cada uno de las grandes divisiones de un programa de computador.

**Morbilidad:** mide la frecuencia de enfermedad en una población específica. Se expresa como incidencia y prevalencia.

**Reportes:** documento impreso o digital de una acción realizada por una persona o máquina.

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

**Operario:** persona que hacen uso de los recursos de cómputo e informáticos.

**Pago capitado:** es una herramienta de gestión que permite operar sobre el gasto y sobre las conductas de las personas. El estado contrata un prestador de servicios médicos para sus afiliados al cual se le paga un monto estipulado por afiliado y por mes, atiendan los afiliados que atiendan, siempre se paga un monto fijo por cada afiliado.

**Política de seguridad:** intención y dirección general expresada formalmente por la dirección. Documentos que establecen el compromiso de la dirección y el enfoque de la organización en la gestión de seguridad de información.

**POS:** el plan obligatorio de salud subsidiado (pos-s), es el paquete de servicios de salud a los que tienen derecho los afiliados al régimen subsidiado, según la normatividad vigente en el sistema de seguridad social en salud en Colombia. Este plan, contempla diferentes actividades, intervenciones y procedimientos de salud que están clasificados según su nivel de atención y complejidad, el plan de

beneficios está relacionado más adelante de conformidad a cada nivel de complejidad.

**Proceso:** conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

**Programa:** secuencia de instrucciones que obliga al computador a realizar una tarea determinada.

**Proveedor de servicios:** profesional que presta servicios a la cartera de clientes de alguna empresa.

**Riesgo:** combinación de la probabilidad de un evento y sus consecuencias. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**Satisfacción de los beneficiarios:** bienestar de los pacientes frente al nivel técnico de la atención, las características de la interacción social con el personal de salud y las condiciones del espacio en el que se brinda la atención. Se incluyen dimensiones ambientales, institucionales, la forma de pago y el costo de la atención recibida. El núcleo central de la valoración termina residiendo en la satisfacción que se genera en una interacción social, en la integralidad del trato personal.

**Sistema de salud:** conjunto de elementos que interactúan para producir salud.

**Servidor:** computador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los computadores que se conecten con él para dicho fin.

**Sismed:** es el sistema de información que apoya el proceso de regulación de precios de medicamentos. Su función es controlar de manera efectiva el incremento de los precios a través de la cadena de comercialización.

**Sistema general de seguridad social en salud (sgsss):** regula el servicio público esencial de salud y crear condiciones de acceso para toda la población residente del país, en todos los niveles de atención.

**Software:** componentes inmateriales del computador como programas, sistemas operativos, etc.

**TI:** tecnologías de Información.

**Vulnerabilidad:** debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

# INTRODUCCIÓN

A finales del siglo XX, los sistemas informáticos se han constituido en herramientas poderosas para administrar los procesos más importantes de una empresa, sus sistemas de información y la misma información. Debido al auge de la informática y a la gran incidencia en el *business management* (manejo empresarial), se han efectúan auditorías con el fin de asegurar la eficiencia de las organizaciones, así como la confiabilidad y seguridad de sus sistemas de información.

La IPS Indígena Guaitara del municipio de Ipiales es una entidad pública de carácter especial autorizada y vigilada por la superintendencia de salud, comprometida con la salud, progreso y desarrollo de la comunidad de los resguardos de Ipiales, Yaramal y San Juan, que ha hecho uso eficiente de los beneficios tecnológicos, renovando tanto hardware como software, para la puesta en marcha de un sistema de información de alta calidad que permite brindar un mejor servicio a sus beneficiarios.

La auditoría de sistemas abordada en este trabajo consiste en planificar, preparar y realizar una revisión al software de administración y gestión de información INFO-SALUD utilizado en la IPS Indígena Guaitara en el municipio de Ipiales y el grado de cumplimiento de los objetivos de este software.

En aras del mejoramiento continuo se hace indispensable planificar, preparar y realizar una auditoría al software de administración y gestión de información INFO-SALUD en funcionamiento utilizada en la IPS Indígena Guaitara en el municipio de Ipiales y el grado de cumplimiento de los objetivos planteados por esta aplicación con el fin de determinar su confiabilidad y lograr cumplir las expectativas de los directivos, operadores del sistema y principalmente de los beneficiados por los servicios gestionados por este software.

La auditoría a los módulos que integran el software de administración y gestión de información INFO-SALUD ha permitido conocer el grado de eficiencia y eficacia en el uso y almacenamiento de la gestión de información en la IPS Indígena Guaitara.

Este trabajo de grado titulado “Auditoría de Sistemas Aplicada a los Módulos de Facturación, Consultas e Historia Clínica del Software INFO-SALUD en la IPS Indígena Guaitara del Municipio de Ipiales” está enmarcado en la línea de gestión y control, específicamente corresponde a la temática de Auditoría de Sistemas se aplica particularmente al software de administración y gestión de información INFO-SALUD montado en la IPSI Guaitara del municipio de Ipiales.

Este trabajo corresponde a la modalidad de trabajo de aplicación, modalidad estipulada por el acuerdo N° 005 de 2010 emanado por el Honorable Consejo Académico de la Universidad de Nariño.

Para entender la problemática que respalda la realización de este trabajo se tiene que la IPS Indígena Guaitara del municipio de Ipiales es una institución prestadora de servicios de salud pública de carácter especial que ofrece sus servicios principalmente a las comunidades indígenas de los resguardos de Ipiales, San Juan y Yaramal, con equidad, solidaridad y humanismo promoviendo el respeto a su estilo de vida, a su integridad étnica, a sus creencias y a sus valores socioculturales;

Debido a la gran importancia que implica la prestación de servicios de salud pública de esta IPSI en la comunidad, es trascendental que en los procedimientos de esta entidad se garantice la integridad, seguridad y claridad en la información suministrada.

Uno de los elementos importantes dentro de la administración de la IPS Indígena Guaitara es su software de gestión de información INFO-SALUD compuesto por los módulos de facturación (manejo de kardex, inventario de medicamentos e insumos, procesos), historia clínica (odontología, medicina general, post consulta) y consultas (información general de códigos de pacientes, convenios, farmacia),

La ejecución de la auditoría se llevó a cabo sobre los módulos de facturación historia clínica y módulo de consulta del software de gestión de información INFO-SALUD implementado en la IPS indígena Guaitara. La base de datos está en Microsoft Access y su interfaz de usuario está desarrollada en Visual Basic.

Se encontró que la falta de una auditoría a este software no ha permitido identificar el porqué de problemas como pérdidas de auditoría historias clínicas y pérdida de registro de medicamentos en el módulo de facturación, es así como en aras del mejoramiento continuo en la prestación de servicios a los beneficiarios, se hizo indispensable una auditoría a los módulos que conforman el software de gestión de información INFO-SALUD con el fin de determinar su confiabilidad mediante el análisis y evaluación que permitió detectar amenazas que afectan la eficiencia de los servicios ofrecidos por la IPS indígena Guaitara.

La falla del software de administración y gestión de información INFO-SALUD o uno de los módulos que lo conforman llevan a la congestión de trabajo manual ocasionando pérdida de tiempo y una deficiente atención al beneficiario, siendo la razón de existir de la entidad.

En consecuencia, se estableció como pregunta principal la siguiente: ¿Cómo la aplicación de una auditoría ayudará a establecer el grado de confiabilidad e integridad de la información en los módulos de facturación, consulta e historia clínica del software de gestión de información INFO-SALUD montado en la IPS Indígena Guaitara de la ciudad de Ipiales?

En este orden de ideas, se identificaron las siguientes inquietudes conductoras del trabajo:

- ¿Cómo se puede detectar las vulnerabilidades, amenazas y riesgos en los módulos pertenecientes al sistema de administración y gestión INFO-SALUD implementado en la IPS Guaitara del municipio de Ipiales?

- ¿De qué forma se puede evidenciar las fallas en el software INFO-SALUD con respecto a la funcionalidad, confiabilidad y disponibilidad de la información?

- ¿Cómo determinar las posibles causas que originan las fallas para establecer respectivas recomendaciones que permitan a la empresa generar controles con el fin de mitigar vulnerabilidades, amenazas y riesgos encontrados?

- ¿Cómo las recomendaciones permitirán a la empresa generar controles con el fin de mitigar vulnerabilidades, amenazas y riesgos encontrados?

Una vez concretado el hilo conductor, se determinó como objetivo general el siguiente:

“Establecer el grado de confiabilidad e integridad de la información de los módulos de facturación, consultas e historia clínica perteneciente al software de gestión de información INFO-SALUD montado en el servidor de la IPS Indígena Guaitara, y dar las recomendaciones pertinentes”.

Para lograr el cumplimiento del objetivo general se definieron los siguientes objetivos específicos:

- Realizar una evaluación de vulnerabilidades, amenazas y riesgos de los módulos del software que maneja la facturación, consulta e historia clínica de la IPSI Guaitara.

- Aplicar técnicas de auditoría que permitan evidenciar vulnerabilidades en el software INFO-SALUD con respecto a la confiabilidad e integridad de la información.

- Determinar las posibles causas que originan las fallas para establecer respectivas recomendaciones que permitan a la empresa generar controles con el fin de mitigar vulnerabilidades, amenazas y riesgos.

- Elaborar recomendaciones que permitan a la empresa generar controles con el fin de mitigar vulnerabilidades, amenazas y riesgos encontrados.

Así mismo, para dar cumplimiento a los objetivos, este trabajo tiene la siguiente justificación.

La Auditoría de Sistemas, hoy en día es de vital importancia para las empresas ya que si no se prevé los mecanismos de control, seguridad y respaldo de la información dentro de una institución, esta se verá sometida a riesgos lógicos, físicos y humanos, que conlleva a perjuicios económicos, de información y de prestación de servicio a los beneficiarios de la asistencia prestada por las instituciones.

La auditoría de sistemas aplicada a los módulos de facturación, historia clínica y consulta, pertenecientes al software de gestión de información INFO-SALUD es de importancia para la institución prestadora de servicios ya que permitió mediante la investigación, revisión y evaluación de procesos gestionados por el software anteriormente mencionado; detectar posibles inconvenientes en funcionamiento y calidad de la información. Una vez analizados los diferentes procedimientos realizados por el software se procedió a emitir las respectivas recomendaciones que permitió una utilización más eficiente de la información, logrando así un mayor nivel de confianza, un mejor nivel de seguridad y optimización de los procesos que en el contexto laboral de la IPS Indígena Guaitara mejoró la prestación de servicios a beneficiarios, operarios y administradores del sistema.

Con la ejecución de esta auditoria se ve beneficiada la IPS GUAITARA, ya que se logró una visión del origen de los inconvenientes presentados, como afrontarlos y como prevenir futuros errores, a través de las respectivas recomendaciones propuestas, permitiendo que la entidad logre:

- Confiabilidad de la información
- Mejora en la prestación del servicio
- Evitar inconvenientes que pueden afectar la operación e integridad de la organización.

El alcance del trabajo de auditoría de sistemas implica la evaluación de los módulos de facturación, consulta e historia clínica del software INFO-SALUD.

Específicamente se evaluaron los siguientes aspectos en la auditoría:

- Documentación básica del sistema informático, como los respectivos manuales de procedimientos, de usuario y de análisis.

- Licenciamiento: Se evaluará el cumplimiento de la documentación de adquisición del software.

- Efectividad del Sistema: Analizar el grado de satisfacción y confiabilidad del sistema informático con el fin de evaluar la precisión de la información.

- Procesos de respaldo: Evaluar procesos y tiempos de *backups* o copias de respaldo de la información.

- Cumplimiento de los requisitos de cliente: Se evaluarán las necesidades y requerimientos que se tuvieron en cuenta para la adquisición del software.

Para el proceso de auditoría se utilizó el estándar COBIT como una metodología de buenas prácticas en el uso de las tecnologías de información, y como el estándar más completo para evaluación de riesgos y cumplimiento de objetivos de control informático a nivel mundial.

# 1. MARCOS

## 1.1 MARCO REFERENCIAL

Los trabajos de grado detallados a continuación son trabajos de auditoría que se toman como referencia y se han tenido en cuenta para el desarrollo del presente trabajo; permitiendo así contextualizar mejor temáticas y metodologías de auditoría aplicadas a sistemas de información en otras instituciones con resultados exitosos.

- **TÍTULO DEL TRABAJO:** AUDITORÍA DEL MÓDULO DE HISTORIA CLÍNICA ELECTRÓNICA DEL SISTEMA DE INFORMACIÓN EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**.**

  **UNIVERSIDAD DE NARIÑO**

  **AUTORES DEL TRABAJO:** JENNY NAYIBI BURGOS – MARÍA CAROLINA DOMÍNGUEZ.

  **OBJETIVO GENERAL:** Evaluar el proceso y el módulo de historias clínicas electrónicas, que garanticen la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del Hospital Universitario Departamental de Nariño.

  El trabajo es tomado como referencia puesto que este trabajo evalúa el proceso de entrada, salida y procesamiento de datos; estableciendo controles y recomendaciones a esta institución de salud.

  **CONCLUSIONES**

  La aplicación de esta auditoría permite reducir los riesgos, favorecer la protección de los recursos de una empresa, mayor comprensión de la información y de los procesos, proporcionar recomendaciones con el ánimo de aportar en la soluciones de los problemas que se presenten.

  Entre los aspectos negativos de una auditoría están: el personal de una organización es reacia a entregar información por desconocimiento de lo que es verdaderamente una auditoría, lo que lleva a que el auditor deba interpretar de la mejor manera posible el funcionamiento de los procesos de una entidad con los recursos que se le entregan.

Al aplicar esta auditoría se obtuvo como experiencia: que debe existir buena comunicación entre las personas auditadas y el auditor para poder tener una buena comprensión de lo que está sucediendo en la organización, la aclaración de algunos conceptos aprendidos en el área de auditoría, además nos permitió conocer a una de las entidades de salud más importantes del departamento de Nariño

- **TÍTULO DEL TRABAJO:** AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUAITARA DEL MUNICIPIO DE IPIALES.

  **UNIVERSIDAD DE NARIÑO**

  **AUTORES DEL TRABAJO:** JULIO CÉSAR BURGOS - NELSON ANDRÉS CORTÉS BERNAL

  **OBJETIVO GENERAL:** APLICAR TÉCNICAS DE AUDITORÍA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUAITARA QUE CONTRIBUYAN A EVIDENCIAR VULNERABILIDADES EN LA SEGURIDAD FÍSICA Y LÓGICA A LOS QUE SE ENCUENTRA EXPUESTA.

  Mediante este trabajo se puede conocer aspectos relacionados con la empresa, en tanto que evalúa su seguridad física y lógica a nivel general en la organización, permitiendo entender que todo funciona como un sistema y lo que afecte a un componente afectará a la organización.

  **CONCLUSIONES**

  En la IPS Indígena Guaitara existen muchas deficiencias en relación a la seguridad física y lógica de los recursos de TI, ya que los procesos que se encuentran establecidos en la entidad no son los suficientes para determinar que se encuentren en un óptimo desempeño ocasionando el no cumplimiento de los objetivos.

  En la IPS Indígena Guaitara la información se encuentra expuesta a muchos riesgos a lo largo de todo su manejo, desde que es generada, hasta que es almacenada. Es por eso que la entidad debe establecer políticas de seguridad de tipo lógico y físico. Ambas de la misma importancia para conservar a la información de forma segura.

**Reseña explicativa del software INFO-SALUD.** En la IPS Indígena Guaitara desde el año 2010 se viene manejando el software de administración y gestión INFO-SALUD, que utiliza la arquitectura cliente-servidor y permite gestionar la información de los aspectos asistenciales, consulta externa, administrativos y contables de entidades públicas y privadas prestadoras de servicios de salud.

Los módulos principales del software INFO-SALUD, son:

- HistoriaNet
- Citas Médicas
- Facturación
- Kardex

## 1.2 MARCO TEÓRICO

**1.2.1 Auditoría.** Conceptualmente la auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas[1].

Según Mario Piattini Velthuis, la auditoría informática es "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos"[2].

Con frecuencia la palabra auditoría se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a utilizar la palabra "auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio, no sólo detecta errores, sino que es un examen técnico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo[3].

[1] AYALA, Magno, Controles Generales, 2001, http://www.monografias.com/trabajos11/codif/codif.shtml [Consulta: 15 de Diciembre de 2014]
[2] PIATTINI, Mario. Auditoria de tecnologías y sistemas de información. Pág. 7
[3] CORTEZ Claudia. Auditoría Informática, 2008, http://claudiacortezrocha.blogspot.com.co/2008/10/auditora-informtica_24.html [Consulta: 15 de Diciembre de 2014]

Así como existen normas y procedimientos específicos para la realización de auditorías contables, existen también normas y procedimientos para la realización de auditorías en informática como parte de una profesión; estas pueden estar basadas en las experiencias de otras profesiones pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución[4].

**1.2.2 Auditor.** Se refiere a la persona capacitada y experimentada que se designa por una autoridad competente o por una empresa de consultoría, para revisar, examinar y evaluar con coherencia los resultados de la gestión administrativa y financiera de una dependencia o entidad con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño[5].

**1.2.3 Tipos de auditoría.** Existen algunos tipos de Auditoría entre las que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática[6].

**a) Auditoría externa**

Es el examen realizado para expresar un criterio profesional sobre el funcionamiento y eficiencia que tiene una organización en el desarrollo de una determinada gestión, este trabajo lo elabora personal independiente, ya sea que trabaje en forma lucrativa o no.

El objetivo de la auditoría externa es emitir una opinión sobre la razonabilidad, integridad y autenticidad de los estados, expedientes y documentos y toda aquella información producida por los sistemas de una organización.

La auditoría externa debe seguir los siguientes procedimientos específicos:

- Identificar riesgos (Negocio, Fraude y Procesos)
- Evaluar su susceptibilidad a distorsiones (errores) en la información.

[4] Ibíd.
[5] WALES, Jimmy y SANGER, Larry. Auditor, < https://es.wikipedia.org/wiki/Auditor> [Consulta: 15 de Diciembre de 2014]
[6] HISPAVISTA, Tipos de Auditoría [en línea], <http://anaranjo.galeon.com/tipos_audi.htm> [Consulta: 15 de Diciembre de 2014]

- Diseñar procedimientos de auditoría que permitan evaluar el diseño, la implementación y efectividad de los controles implementados.

- Diseñar procedimientos de auditoría sustantivos de acuerdo con la evaluación de los riesgos[7].

**b) Auditoría interna**

El Instituto de Auditores Internos de los Estados Unidos define la Auditoría Interna como: "La auditoría interna es una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección".[8]

La auditoría interna surge por la necesidad de mantener un control permanente y eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, se ocupa fundamentalmente del sistema de control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger sus activos, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera[9].

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección[10].

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades proporcionándoles objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas[11].

---

[7] MAILXMAIL Redactores, Auditoría interna y externa. Definición y características, http://www.mailxmail.com/auditoria-interna-externa-definicion-caracteristicas_h, [Consulta: 15 de Diciembre de 2014]

[8] LEFCOVICH, Mauricio León, Auditoría Interna, http://www.gerencie.com/auditoria-interna.html, [Consulta: 15 de Diciembre de 2014]

[9] MLEFCOVICH, Auditoría interna. Un enfoque sistémico y de mejora continua, http://www.monografias.com/trabajos15/auditoria-interna/auditoria-interna.shtml, [Consulta: 15 de Diciembre de 2014]

[10] Ibíd.

[11] Ibíd.

**1.2.4 Enfoques de auditoría.** Entre los principales tipos de Auditoría se tiene los siguientes:

- Auditoría financiera: 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[12].

- Auditoría administrativa: revisa y evalúa si los métodos 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[13].

- Auditoría operacional: se centra en la medición de la posición financiera, de los resultados de las operaciones y de los flujos de efectivos de una entidad, una auditoría operacional se centra en la eficacia, la eficiencia y la economía de las operaciones. El auditor operacional evalúa los controles operativos de la administración y de los sistemas sobre actividades tan diversas como las compras, procesamiento de datos, recepción, envió, servicios de oficina, publicidad, entre otros.

- Auditoría gubernamental: es la revisión y examen que llevan a cabo las entidades fiscalizadoras superiores a las operaciones de diferente naturaleza, que realizan las dependencias y entidades del gobierno central, estatal y municipal en el cumplimiento de sus atribuciones legales[14].

- Auditoría integral: la auditoría integral es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la siguiente temática: la Información financiera, la estructura del control interno, el cumplimiento de las leyes pertinentes y la conducción ordenada en el logro de las metas y objetivos propuestos; con el propósito de informar sobre el

[12] MARIN, Hugo Armando. Auditoría financiera, http://www.gerencie.com/auditoria-financiera.html, [Consulta: 15 de Diciembre de 2014]
[13] Ibíd.
[14] SALAS, Alejandra, Auditoría Gubernamental.pdf, 2011, http://www.uv.mx/personal/alsalas/files/2015/05/Auditoria-Gubernamental.pdf, [Consulta: 15 de Diciembre de 2014]

grado de correspondencia entre la temática y los criterios o indicadores establecidos para su evaluación[15].

- Auditoría de sistemas: 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[16].

### 1.2.5 Auditoría de sistemas

#### Concepto de auditoría de sistemas

La auditoría de sistemas se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, se señalaran algunos aspectos básicos para su entendimiento[17].

Así, la auditoría de sistemas es:

1. Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleve a cabo de una manera oportuna y eficiente.

2. Las actividades ejecutadas por los profesionales del área de Informática y de auditoría encaminada a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual ha de contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y la optimización permanente de la tecnología de informática en el negocio.

---

[15] CUÉLLAR, Guillermo, Auditoría Integral, http://preparatorioauditoria.wikispaces.com/Marco+Conceptual+de+la+Auditoria+Integral [Consulta: 15 de Diciembre de 2014]

[16] PARRA , Andres, Auditoría de Sistemas de Información, 2008, http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html [Consulta: 15 de Diciembre de 2014]

[17] MORENO, Lorena, La auditoría en la informática, 2003, http://es.slideshare.net/MOSHERG/auditoria-informatica-tesis, [Consulta: 15 de Diciembre de 2014]

3. El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que pasa por el área se manejan con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

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

De este modo la auditoría de sistemas sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos
  .
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

**1.2.6 Auditoría de sistemas como objeto de estudio.** Se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información[18]

Objetivo de un auditor de sistemas: brindar recomendaciones a la alta gerencia para mejorar o lograr un adecuado control interno en ambientes de tecnología informática con el fin de lograr mayor eficiencia operacional y administrativa.

[18] Castañón, Blanca, 2012, Auditoría de sistemas de información. http://www.gestiopolis.com/auditoria-de-sistemas-de-informacion/[Consulta: 15 de Diciembre de 2014]

## 1.3 METODOLOGÍA DE AUDITORÍA DE SISTEMAS

**1.3.1 Tipo de investigación**. Este trabajo, teniendo en cuenta la guía de elaboración de trabajo de grado manejada en la facultad de Ingeniería de la Universidad de Nariño, se enmarca dentro del tipo descriptivo-aplicativo, ya que precisa las características más importantes del software INFO-SALUD. Es descriptiva, porque se obtuvo información completa y exacta del funcionamiento de los procesos administrados por este software así como sus entradas y salidas de datos, por lo tanto, basados en técnicas como la seguridad y análisis de integridad de datos se buscó generar un informe de posibles riesgos que se hayan observado.

### 1.3.2 Población y muestra

- Población o Universo

  Víctor Morlés, refiere la población como "el conjunto para el cual serán válidas las conclusiones que se obtengan: a los elementos o unidades (personas, instituciones o cosas) involucradas en la investigación"[19].

  En este sentido se debe entender que la población es el conjunto que tiene una o varios atributos comunes y sobre el que se está interesado en obtener conclusiones, ejemplos: estudiantes de la Universidad de Nariño, los habitantes de la ciudad de Pasto en el presente año, etc.

- Muestra

  Víctor Morlés define la muestra como "subconjunto representativo de un universo o población"[20].

  La Muestra es parte de la población que se analiza, con el objeto de obtener información acerca de toda la población, ejemplos: estudiantes de Ingeniería de Sistemas de la Universidad de Nariño, los habitantes del barrio la Colina de la ciudad de Pasto en el presente año, etc.

[19] MORLES, Víctor. (1994). Planeamiento y análisis de investigaciones. Eldorado Ediciones. Caracas. Venezuela.
[20] Ibíd.

**1.3.3 Aspectos de la evaluación.** Se denomina evaluación al proceso dinámico a través del cual e indistintamente, una empresa, organización o institución puede conocer sus propios rendimientos, especialmente sus logros y flaquezas y así reorientar propuestas o bien focalizarse en aquellos resultados positivos para hacerlos aún más rendidores[21].

La evaluación permite evaluar documentación e información de cara a recolectar evidencias necesarias para reconocer el entorno a evaluar, la población, muestra, procesos y procedimientos del objetivo a auditar y se divide en los siguientes aspectos:

- La documentación del sistema: revisar la situación en que se encuentra toda la documentación básica del sistema, como los manuales de procedimientos, de usuario y de análisis y si están acordes con las necesidades de la dependencia.

- Operatividad del sistema: se debe evaluar que el sistema efectúe en cada etapa de su ciclo las especificaciones establecidas en el Análisis y Diseño y se cumpla con el procedimiento aprobado para el sistema. Debe analizarse y observar también, si realmente tiene los requisitos de operatividad que hagan al sistema eficiente y eficaz.

- Ciclo de vida: se debe revisar todo el ciclo del sistema:

    - Generación del dato
    - Ingreso del dato
    - Transmisión del dato
    - Procesamiento del dato

- Actualización de archivos: debe evaluarse que existan registros y rutinas de control que con cierta frecuencia de tiempo o de período, determine si existe coherencia entre la cantidad de registros y valores de totales de los archivos.

- Integridad de los datos: establecer procedimientos de comparación de la información producida por el sistema contra otras informaciones disponibles, para efectos de determinar la confiabilidad de la información.

[21] DEFINICION ABC, Definición de evaluación, http://www.definicionabc.com/general/evaluacion.php[Consulta: 16 Septiembre de 2015]

Un aspecto importante de todo el sistema son los resultados, por lo que al revisar el sistema debe evaluarse que los resultados cumplan con las especificaciones del diseño del sistema, lo cual debe comprobarse mediante juegos de datos de pruebas especialmente preparados, y que prueben todas las posibilidades de las entidades, datos y situaciones.

- Efectividad del sistema: otro aspecto importante del sistema, es que sea efectivo en conseguir los objetivos y beneficios esperados, por lo que se debe indagar a los operarios sobre el grado de satisfacción y confiabilidad del sistema, que beneficios han sido conseguidos y los motivos que impiden lograr otros, si los costos de operación del sistema se encuentran dentro de lo planificado y que mejoras se han conseguido con tal reducción, que tanto ha mejorado la precisión de la información y en qué medida se ha completado y básicamente, cuánto se redujo el tiempo de atención al cliente y cuál fue el incremento de productividad para la institución poseedora del mismo.

- Seguridad del sistema: debe comprobarse que el sistema cuente con los siguientes tipos de seguridad:

  ✓ Seguridad de acceso a la información

  ✓ Seguridad de acceso a los programas

  ✓ Seguridad ante contaminación de virus

- Sistema de respaldo: previendo posibles problemas con el software es necesario que el equipo central cuente con características técnicas de respaldo como listados diarios de información, lo cual permitiría seguir operando por lo menos manualmente en casos extremos.

- Backups de la base de datos: deberían efectuarse por cada cambio de turno de trabajo o como mínimo al final del día, debiendo inclusive el sistema haber sido programado para que exija efectuar el backup respectivo.

- Copia de respaldo de los programas fuentes y objetos de las aplicaciones, de la plataforma de software y de las bases de datos completas de la Institución (hasta de tres períodos anteriores), debiéndose guardar una copia en el local de la Institución y otra adicional en otro local para afrontar siniestros o desastres que pudieran ocurrir.

- Auditabilidad del sistema: en general, todo sistema que se encuentra instalado, debe contar con volúmenes de información como:

- ✓ Manual de usuario del software
- ✓ Manual de procedimientos de los sistemas
- ✓ Descripción genérica
- ✓ Diagramas de entrada, archivos, salida
- ✓ Salidas
- ✓ Fecha de instalación de los sistemas
- ✓ Proyecto de instalación de nuevos sistemas

**1.3.4 Recolección de información para auditoría de sistemas.** Las técnicas de recolección de información son procedimientos especiales utilizados para obtener y evaluar las evidencias necesarias, suficientes y competentes que le permitan formar un juicio profesional y objetivo, que facilite la calificación de los hallazgos detectados en la materia examinada. El actor debe seleccionar la técnica más apropiada, para examinar cualquier operación, actividad, área, programa, proyecto o transacción de la entidad bajo examen[22].

Las técnicas de recolección de datos, pueden ser:

- **Observación**

  Permite recolectar la información directamente sobre las funciones, actividades, procedimientos y operación de los sistemas; se aplica para observar todo lo relacionado con los sistemas de una organización con el propósito de percibir, examinar, o analizar los eventos que se presentan en el desarrollo de las actividades del área o de un sistema que permita evaluar el cumplimiento de las funciones, operaciones y procedimientos[23].

- **Entrevistas**

  Es un medio directo para la recolección de información por medio de grabadoras digitales o cualquier otro medio. En la entrevista, el auditor

[22] GARCÍA, Daynelis, Anexo II. Técnicas de Recolección de Información, http://www.eumed.net/libros-gratis/2010f/852/TECNICAS%20DE%20RECOLECCION%20DE%20INFORMACION.htm, [Consulta: 15 de Diciembre de 2014]

[23] SOLARTE, Nicolás, Recolección de información para auditoría informática y de sistemas, 20011, http://auditordesistemas.blogspot.com.co/2011/11/recoleccion-de-informacion-para.html, [Consulta: 15 de Diciembre de 2014]

interroga, investiga y conforma directamente sobre los aspectos que se está auditando con el fin de profundizar y preguntar sobre el tema a auditar.

Esta técnica permite obtener información sobre lo que está auditando, además de aspectos importantes que permitirán conocer más sobre las funcionalidades que se van a analizar[24].

- **Cuestionarios**

Los cuestionarios son preguntas impresas en formatos o fichas en que el auditado responde de acuerdo a su criterio, de esta manera el auditor obtiene información que posteriormente puede clasificar e interpretar por medio de la tabulación y análisis, para evaluar lo que se está auditando y emitir una opinión sobre el aspecto evaluado[25].

- **Encuestas**

Las encuestas son utilizadas frecuentemente para recolectar información sobre aspectos como el servicio, el comportamiento y utilidad del equipo, la actuación del personal y los operarios, entre otros juicios de la función informática. No existen reglas para el uso de las encuestas, solo los que regulan los aspectos técnicos y estadísticos tales como la elección del universo y la muestra, que se contemplan dentro de la aplicación de métodos probabilísticas y estadísticos para hacer la mejor elección de las muestras y recolección de opiniones[26].

- **Archivo permanente**

El archivo permanente reúne los datos de naturaleza histórica o continua de la entidad. Estos archivos proporcionan una fuente conveniente de información para posteriores auditorías, estos documentos están conformados por reglamentos, contratos, manuales de funciones, instructivos y normas.

El archivo permanente se refiere a la información que es válida en el tiempo. Este archivo debe suministrar al equipo auditor la información sobre la entidad con el fin de llevar una auditoría eficaz y objetiva[27].

---

[24] Ibíd.
[25] Ibíd.
[26] SOLARTE, Nicolás, Recolección de información para auditoría informática y de sistemas, 20011, http://auditordesistemas.blogspot.com.co/2011/11/recoleccion-de-informacion-para.html, [Consulta: 15 de Diciembre de 2014]
[27] ALVARADO, Tello, Conformacion del archivo permanente, http://www.academia.edu/9181126/Papeles_de_Trabajo [Consulta: 1 Febrero de 2015]

**1.3.5 Marco de referencia COBIT**. COBIT es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. COBIT enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT[28].

El propósito de COBIT es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan. COBIT permite entender cómo dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. COBIT suministra las herramientas para supervisar todas las actividades relacionadas con TI.

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporción en la información que la empresa necesita para alcanzar sus objetivos.

COBIT se divide en tres niveles:

- Dominios: agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

- Procesos: conjuntos o series de actividades unidas con delimitación o cortes de control.

- Actividades: acciones requeridas para lograr un resultado medible.

Se definen 34 objetivos de control generales, para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios[29].

**Dominio: planear y organizar (PO)**

Este dominio cubre la estrategia y las 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

[28] CAMELO, Leonardo, Qué es COBIT?, 2010,http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html [Consulta: 15 de Diciembre de 2014]
[29] PÉREZ, Luz, Estrategia, 2015,http://estrategiasdegestionservicios.blogspot.com.co/2015/03/24-ventajas-y-desventajas[Consulta: 20 de Abril de 2015]

necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas[30].

Los procesos del dominio planear y organizar (PO), son:

**PO1 Definición de un plan estratégico:** la planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI[31].

**PO2 Definición de la arquitectura de información:** la función de los sistemas de información debe crear y actualizar de forma segura un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contenga las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales, asegurándose de proporcionar información fiable y segura[32].

**PO3 Determinación de la dirección tecnológica:** la función de los servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones[33].

**PO4 Definición de la organización y de las relaciones de TI:** una organización de TI se debe definir tomando en cuenta los requerimientos de personal,

[30] UNAM, 2009, Sitio Web de Seguridad Para TI Basado en Cobit, http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_aplicativa/dominios.html [Consulta: 20 de Diciembre de 2014]
[31] ISACA, COBIT 4.1, Estados Unidos, 2007, Pág. 29
[32] ibíd. Pág. 33
[33] ibíd. Pág. 37

funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, deben determinar las prioridades de los recursos TI alineados con las necesidades del negocio[34].

**PO5 Manejo de la inversión:** establecer y mantener un marco de trabajo para administrar los programas de inversión TI que abarquen los costos, beneficios y prioridades dentro del presupuesto[35].

**PO6 Comunicación de la dirección y aspiraciones de la gerencia:** la dirección debe elaborar un marco de trabajo de control empresarial TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos a probados y apoyados por la dirección. La comunicación apoya el logro de los objetivos TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes[36].

**PO7 Administración de recursos humanos:** adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logró siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal[37].

**PO8 Administrar la calidad:** se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad[38].

**PO9 Evaluación de riesgos: c**rear y dar mantenimiento a un maro de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos TI, estrategias y mitigación de riesgos residuales[39].

---

[34] ibíd. Pág. 41
[35] ibíd. Pág. 47
[35] ibíd. Pág. 51
[36] ibíd. Pág. 55
[37] ibíd. Pág. 58
[38] ibíd. Pág. 63
[39] ibíd. Pág. 67

**PO10 Administración de proyectos:** establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. Se debe tener en cuenta un plan que contenga asignación de recursos, definición de entregables, aprobación de los operarios, un enfoque de entrega por fases, aseguramiento de calidad, un plan formal de pruebas y post implantación[40].

**Dominio: adquirir e implementar (AI)**

Para llevar a cabo la estrategia de TI, las soluciones 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[41].

Los procesos del dominio adquirir e implementar (AI), son:

**AI1 Identificación de soluciones automatizadas:** la necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de "desarrollar" o "comprar"[42].

**AI2 Adquisición y mantenimiento del software aplicativo:** las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, además del desarrollo y la configuración[43].

**AI3 Adquisición y mantenimiento de la infraestructura tecnológica:** las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio[44].

---

[40] ibíd. Pág. 67
[41] UNAM, 2009, Sitio Web de Seguridad Para TI Basado en Cobit, http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_aplicativa/dominios.html[Consulta: 20 de Diciembre de 2014]
[42] ISACA, COBIT 4.1, Estados Unidos, 2007, Pág. 73
[43] ibíd. Pág. 77
[44] ibíd. Pág. 83

**AI4 Facilitar la operación y es uso:** el conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura[45].
**AI5 Facilitar la operación y el uso:** se deben suministrar TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable[46].

**AI6 Administración de los cambios:** todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios se deben registrar, evaluar y autorizar previo a la implantación. Esto garantiza la reducción de riesgos que impactan negativamente a la estabilidad o integridad del ambiente de producción[47].

**AI7 Instalar y acreditar soluciones y cambios:** los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operarios estén en línea con las expectativas convenidas y con los resultados[48].

**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[49].

Los procesos del dominio Entregar y dar Soporte (DS), son:

[45] ibíd. Pág. 85
[46] ibíd. Pág. 89
[47] ibíd. Pág. 89
[48] ibíd. Pág. 97
[49] NAM, 2009, Sitio Web de Seguridad Para TI Basado en Cobit, http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_aplicativa/dominios.html[Consulta: 20 de Diciembre de 2014]

**DS1 Definición de niveles de servicio:** contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los interesados sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios TI y los requerimientos de negocio relacionados[50].

**DS2 Administración de servicios prestados por terceros:** la necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de tercero. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos[51].

**DS3 Administración de desempeño y capacidad:** la necesidad de administrar el desempeño y la capacidad de recursos TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda seguridad de que los recursos de información que soportan los requerimientos del negocio que están disponibles[52].

**DS4 Asegurar el servicio continuo:** la necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua[53].

**DS5 Garantizar la seguridad de sistemas:** la necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las deidades o incidentes de seguridad identificados[54].

---

[50] ISACA, COBIT 4.1, Estados Unidos, 2007, Pág. 101
[51] ibíd. Pág. 105
[51] ISACA, COBIT 4.1, Estados Unidos, 2007, Pág. 109
[52] ibíd. Pág. 113
[53] ibíd. Pág. 117
[54] ibíd. Pág. 121

**DS6 Identificar y asignar costos:** la necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respecto al uso de los servicios TI[55].

**DS7 Educar y entrenar a los usuarios:** para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios[56].

**DS8 Administrar la mesa de servicio y los incidentes:** responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis de causa raíz y resolución. Los beneficios del negocio incluyendo el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo[57].

**DS9 Administrar la configuración:** garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener en repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido[58].

**DS10 Administración de problemas:** una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas

[55] ibíd. Pág. 123
[56] ibíd. Pág. 125
[57] ibíd. Pág. 129
[58] ibíd. Pág. 133

desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la convivencia y satisfacción del usuario[59].

**DS11 Administración de datos:** una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio[60].

**DS12 Administración del ambiente físico:** la protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (*site*), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal[61].

**DS13 Administración de operaciones:** un procesamiento de información completa y apropiada requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI[62].

**Dominio: monitorear y evaluar (ME)**

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para evaluar su calidad y suficiencia en cuanto a los

[59] ibíd. Pág. 137
[60] ibíd. Pág. 141
[60] ibíd. Pág. 145
[61] ibíd. Pág. 149
[62] ibíd. Pág. 149

requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio[63].

Los procesos del dominio Monitorear y Evaluar (ME), son:

**ME1 Monitorear y evaluar el desempeño de TI:** Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas[64].

**ME2 Monitorear y evaluar el control interno efectivo para TI**: requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables[65].

**ME3 Garantizar el cumplimiento con requerimientos externos:** una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumpliendo, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio[66].

**ME4 Proporcionar gobierno de TI:** el establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales[67].

**Ventajas que ofrece COBIT.** COBIT es un marco de referencia aceptado mundialmente de gobierno TI basado en estándares y mejores prácticas de la industria. Una vez implementado, es posible asegurarse de que TI se encuentra efectivamente alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas.

---

[63] UNAM, 2009, Sitio Web de Seguridad Para TI Basado en Cobit, http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_aplicativa/dominios.html [Consulta: 20 de Diciembre de 2014]
[64] ISACA, COBIT 4.1, Estados Unidos, 2007, Pág. 109
[65] ibíd. Pág. 157
[66] ibíd. Pág. 161
[67] ibíd. Pág. 165

Suministra un lenguaje común que permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con auditores TI y otros profesionales.

Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de TI. El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada.

Ayuda a los ejecutivos a entender y gestionar las inversiones en TI a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que TI entregara los beneficios esperados.

Al ser COBIT reconocida y aceptada internacionalmente como una herramienta de gestión, su implementación es un indicativo de la seriedad de una organización. Ayuda a Empresas y profesionales de TI a demostrar su competitividad ante las demás compañías. Así como existen procesos genéricos de muchos tipos de negocios, existen estándares y buenas prácticas específicos para TI que deben seguirse por las compañías cuando se soportan en TI, en donde COBIT agrupa tales estándares y entrega un marco de referencia para su implementación y gestión[68].

**1.3.6 Elementos de auditoría.** Para el proceso de recolección de la información de la auditoría se hace necesario contar con instrumentos de recolección de datos, de ellos depende, en gran medida, la calidad de la información, siendo esta la base para las etapas posteriores y para los resultados.

**Cuadros de fuentes de definición.** Permiten establecer las fuentes de conocimiento (documentación, manual, política o procedimiento) necesarias para la evaluación de un determinado proceso de COBIT, además de definir las pruebas de análisis y ejecución que se deben realizar con dicho material.

Para la elaboración de los cuadros de definición de fuentes de conocimiento se empleó un formato que se muestra en el cuadro 1, este contiene el logo de la entidad auditada y los ítems relacionados como son:

- **REF:** identificación del cuadro de Definición.

- **ENTIDAD AUDITADA:** nombre de la entidad a la cual se le está realizando el proceso de auditoría.

[68] MALDONADO, Mauricio, 2015, Gobierno TI y COBIT, https://prezi.com/mgtzctkknch8/copy-of-gobierno-ti-y-cobit/ [Consulta: 1 Junio de 2015]

- **OBJETO DE ESTUDIO**: identificación de la parte a evaluar

- **RESPONSABLES:** nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

- **MATERIAL DE SOPORTE:** nombre del modelo tomado en la aplicación de la auditoría en este caso COBIT.

- **DOMINIO:** nombre del dominio de COBIT que se está evaluando.

- **PROCESO**: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

- **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** se describe el objetivo del proceso del dominio del COBIT a aplicar.

- **FUENTES DE CONOCIMIENTO:** en este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoría lo que servirá como respaldo del proceso.

- **REPOSITORIO DE PRUEBAS:** se divide en dos tipos de pruebas:

- **DE ANÁLISIS:** describir las pruebas de análisis que se van a realizar para evaluar el proceso específico que se encuentre en estudio.

- **DE EJECUCIÓN:** describir las acciones a realizar para la ejecución de la auditoría, como las revisiones, verificaciones, pruebas y obtención de inconsistencias, etc.

| | | | | | |
|---|---|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORÍA** | | **REF** | | |
| | | | **PLAN** | | |
| **ENTIDAD AUDITADA** | | | **PÁGINA** | | |
| | | | | **DE** | |
| **OBJETO DE ESTUDIO** | | | | | |
| **RESPONSABLES** | | | | | |
| **MATERIAL DE SOPORTE** | | | | | |
| **DOMINIO** | | **PROCESO** | | | |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | | | | | |
| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | | | | |
| | **DE ANÁLISIS** | **DE EJECUCIÓN** | | | |
| | | | | | |

Cuadro 1. Formato definición de fuentes de conocimiento. [1]

**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, donde 1 es un nivel insignificante y 5 un nivel crítico, 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.

Los ítems que se encuentran en este formato, son:

- **REF:** identificación del cuadro de definición.
- **ENTIDAD AUDITADA:** nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- **OBJETO DE ESTUDIO:** identificación de la parte a evaluar
- **RESPONSABLES:** nombres del equipo auditor que está llevando a cabo el proceso de auditoría.
- **MATERIAL DE SOPORTE:** nombre del modelo tomado en la aplicación de la auditoría, en este caso COBIT.
- **DOMINIO:** nombre del dominio de COBIT que se está evaluando.
- **PROCESO:** nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- **PREGUNTA:** listado de preguntas que serán evaluadas.
- **SI, NO Y NA:** posibilidades de respuestas, cumple, no cumple o no aplica para la entidad.
- **FUENTE:** de donde se obtiene la información
- **TOTAL:** se asigna los valores correspondientes a cada columna, la sumatoria de los SI, de los NO y NA.
- **TOTAL CUESTIONARIO:** la suma de los campos de las opciones.

- **PORCENTAJE DE RIESGO:** determina el nivel de riesgo total (riesgo bajo, medio o alto)

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

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

Luego para hallar el porcentaje de riesgo total se calcula así:

$$\%Riesgo\ Total = \ 100 - \%Riesgo$$

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

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

**Riesgo bajo:** las insuficiencias que se exhiben en este nivel no son muy importantes, pero se recomienda considerar soluciones preventivas al largo plazo.

**Riesgo medio:** las insuficiencias que se exhiben en este nivel son de importancia media ya que se puede controlarlo, lo cual permite solucionarlo en un lapso de tiempo determinado.

**Riesgo alto:** las insuficiencias que se exhiben en este nivel son de gran importancia y se deben tomar medidas radicales e inmediatas con el objeto de reducir el riesgo, caso contrario este no permitirá alcanzar los objetivos de la entidad.

Con el fin de formular conclusiones acerca de funcionamiento del proceso evaluado y teniendo en cuenta que esta toma validez con la obtención de pruebas que verifique los resultados de la encuesta se utiliza el formato de cuestionario cuantitativo (ver cuadro 2).

| | | |
|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | **REF** |

| | | | | |
|---|---|---|---|---|
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA DEL MUNICIPIO DE IPIALES** | | **PÁGINA** | |
| | | | **DE** | |
| **OBJETO DE ESTUDIO** | | | | |
| **RESPONSABLES** | | | | |
| **MATERIAL DE SOPORTE** | | | | |
| **DOMINIO** | | **PROCESO** | | |

| **PREGUNTA** | **SI** | **NO** | **NA** | **OBSERVACIÓ** |
|---|---|---|---|---|
| | | | | |
| **TOTAL** | | | | |
| **TOTAL CUESTIONARIO** | | | | |

Cuadro 2. Formato de cuestionario cuantitativo. [1]

**Entrevistas preguntas abiertas y preguntas cerradas**. Técnicas utilizadas para la recolección de información detallada que permite aclarar dudas que dejan los cuestionarios.

Los formatos utilizados para hacer las entrevistas están ajustados a los funcionarios de IPS Indígena Guaitara, quienes están relacionados con la operación de los módulos del software INFO-SALUD.

Para la recolección de la información se realizaron dos tipos de entrevistas:

**Entrevistas con preguntas abiertas:** donde la persona entrevistada puede expresar libremente su respuesta de forma detallada, permitiendo hacer sugerencias según vaya respondiendo cada una.

**Entrevistas con preguntas cerradas:** el entrevistado se limita a contestar "Si" o "No", adicionalmente este tipo de entrevistas permiten anotar observaciones que son útiles para la investigación,

Los formatos de entrevistas se presentan en los cuadros 3 y 4

| **Tipo de Registro: Entrevista I** | | | |
|---|---|---|---|
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA DEL MUNICIPIO DE IPIALES** | | **N° GUÍA** |
| **RESPONSABLES** | | **SISTEMA** | **INFO-SALUD** |
| **OBJETIVO** | | | |
| **RESPONDIDO POR** | | **CARGO** | |
| **R/PT** | | | |
| **FECHA** | | | |
| **N°** | **PREGUNTA** | | |
| | | | |

Cuadro 3. Formato entrevista I. [1]

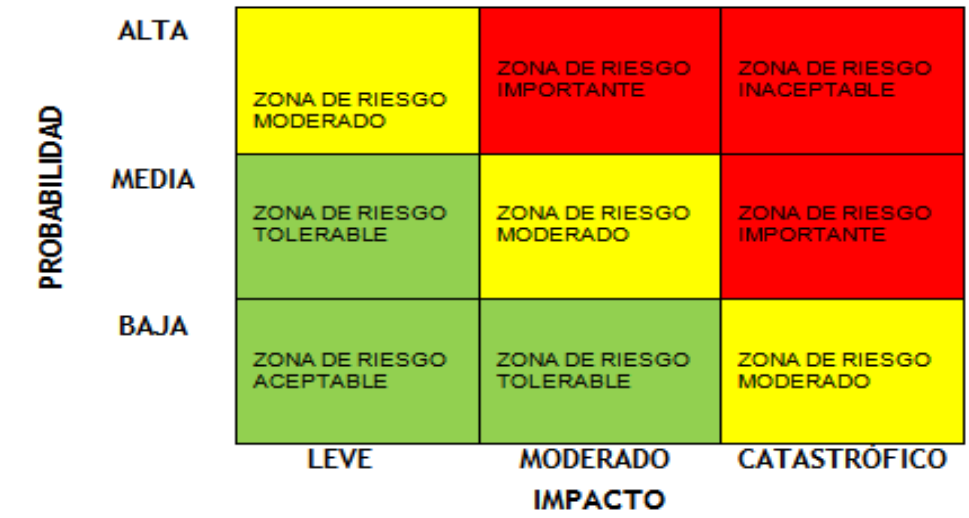
| | | | | | |
|---|---|---|---|---|---|
| | **ENTREVISTA II** | | | **REF** | |
| | | | | | |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** | |
| | | | | **DE** | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | | **PROCESO** | | | |
| | | | | | |
| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** | |
| | | | | | |

Cuadro 4. Formato entrevista II. [1]

**Matriz de probabilidad e impacto.** Una matriz de riesgo de probabilidad de impacto es una representación gráfica de dos dimensiones de los riesgos que enfrenta una organización o entidad, desde un individuo a un planeta entero. La probabilidad de un evento se representa frente a los posibles efectos negativos de ese evento[69].

[69] SIGWEB, MatrizdeRiesgo, http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf [Consulta: 20 de Junio de 2015]

La probabilidad de ocurrencia va en el eje y, en el eje x va el impacto (ver cuadro 5).




Riesgos que necesitan MONITORIZACIÓN: Planes de actuación detectivos.

Riesgos que necesiten INVESTIGACIÓN: Planes de actuación preventivos.

Riesgos que necesitan MITIGACIÓN: Planes de actuación correctivos

Cuadro 5. Formato matriz de probabilidad e impacto. [2]

**Hallazgos.** Un hallazgo es la indicación de la inexistencia o inoperancia de un control. Surge como resultado de la comparación que se realiza entre un criterio y la situación actual encontrada por el auditor.

Teniendo en cuenta la aplicación de los instrumentos para recolección de información, los objetivos planteados con anterioridad y los riesgos definidos en la matriz se obtiene el cuadro de hallazgos (ver cuadro 6).

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | | **PROCESO** | |
| **HALLAZGO** | | | |
| | | | |
| **CONSECUENCIAS** | | | |
| | | | |
| **RECOMENDACIONES** | | | |
| | | | |
| **PROBABILIDAD E IMPACTO** | | | |
| | | | |
| **EVIDENCIAS** | | | |

Cuadro 6. Formato cuadro de hallazgos. [1]

# 2. METODOLOGÍA DE DESARROLLO

La utilización de metodologías es fundamental ya que permite el desarrollo de cualquier tipo de proyectos de forma eficiente y eficaz a través del seguimiento de pasos lógicos.

## PRIMERA ETAPA: RECONOCIMIENTO

1. Visita preliminar a las instalaciones de la IPS Indígena Guaitara con el fin de realizar la observación de los diferentes procesos implementados en esta institución y realización de entrevistas a los funcionarios de los diferentes módulos que componen el software a evaluar, de donde se tomó los siguientes grupos para evaluar:

   ✓ **Población**

   El personal encargado del manejo de los módulos del software INFO-SALUD son 40 personas entre las que están médicos, odontólogos, enfermeras, personal de facturación y personal auxiliar de la IPS Indígena Guaitara.

   ✓ **Muestra**

   La muestra para este trabajo fueron 20 personas representantes de cada uno de los sectores poblacionales que se encargan de la administración de la información manejada en los módulos del software.

2. Estudio y reconocimiento de los módulos de facturación, inventarios e historia clínica (medicina general, odontología y laboratorio) del software de administración y gestión de información INFO-SALUD.

## SEGUNDA ETAPA: PLANEACIÓN DE LA AUDITORÍA

1. Establecer objetivos específicos de la auditoría, metodología, cronograma de actividades y recursos necesarios para implementar el plan de auditoría.

2. Planificación de fases aplicando distintas técnicas de auditoría y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados.

## TERCERA ETAPA: EJECUCIÓN DE LA AUDITORÍA

1. Realización de pruebas de cumplimiento para determinar si los procedimientos están funcionando correctamente.

2. Análisis de riesgos e identificación de las principales vulnerabilidades mediante una matriz de riesgos, elaboración de las tablas de hallazgos, las consecuencias y su respectivo plan correctivo.

## CUARTA ETAPA: DICTAMEN FINAL DE LA AUDITORÍA

1. Elaboración del informe final el cual contiene los procesos evaluados según la actividad a la que está encargado cada módulo, su comportamiento y los hallazgos encontrados con sus respectivas recomendaciones que permitan hacer las correcciones necesarias para su correcto funcionamiento.

2. Este informe se presentó y entregó a la Gerente de la IPS Indígena Guaitara, para que tome las respectivas correcciones a implantar un plan de mejoramiento.

# 3. DESARROLLO DEL TRABAJO

El proceso de auditoría realizado presenta papeles de trabajo que son los documentos en donde se registran los datos, información, pruebas realizadas y los hallazgos obtenidos. Los papeles de trabajo se dividen en dos grupos: archivo permanente y archivo corriente.

## 3.1 ARCHIVO PERMANENTE

Durante el proceso de auditoría las dependencias que facilitaron los documentos para la consecución de este archivo fueron:

- Dirección administrativa dirigida por el Doctor Campo Elías Córdoba.
- Área de sistemas dirigida por el Ingeniero Darío Burbano.
- Dependencia activos fijos.
- Dependencia de auditoría interna dirigida por el médico auditor Dayana Paguay.
- Información obtenida del portafolio de servicios de la IPS Indígena Guaitara.

### 3.1.1 Leyes y decretos comunes

- Ley 100 de 1993

  El sistema de salud en el país depende del Art. 48 de la Constitución Nacional, está reglamentada en el segundo libro de la Ley 100 de 1993 expedida por el Congreso de Colombia, la cual estableció el Sistema de Seguridad Social en Colombia la cual establece reglas fundamentales para regir el servicio público de salud como son la equidad, la obligatoriedad, la protección integral, la libre escogencia, la autonomía de las instituciones, la descentralización administrativa, la participación social, la concertación y la calidad.[70]

[70] ley 100 de 1993, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5248 [Consulta: 1 Febrero de 2015]

- Ley 1122 de 2007

  En la cual se establecen un conjunto de políticas que busca garantizar de manera integrada, la salud de la población por medio de acciones dirigidas tanto de manera individual como colectiva ya que sus resultados se constituyen en indicadores de las condiciones de vida, bienestar y desarrollo.[71]

- Ley 1438 de 2011

  Tiene como objeto fortalecer el SGSSS a través de un modelo de prestación del servicio público en salud que en el marco de la estrategia atención primaria en salud, permita la acción coordinada del estado, IPS, EPS, sociedad para el mejoramiento de la salud y la creación de un ambiente sano y saludable, que brinde servicios de mayor calidad, incluyente y equitativo, donde el centro y objetivo de todos los esfuerzos sean los residentes en el país.[72]

- Decreto 806 de 1998

  Por el cual se reglamenta la afiliación al régimen de seguridad social en salud y la prestación de los beneficios del servicio público esencial de seguridad social en salud y como servicio de interés general, en todo el territorio nacional.

  Este decreto tiene por objeto reglamentar la seguridad social en salud, en todo el territorio nacional, tanto como servicio público esencial como servicio de interés público a cargo de particulares o del propio estado, el tipo de participantes del sistema, la afiliación al régimen de seguridad social en salud y los derechos de los afiliados.[73]

[71] http://www.minsalud.gov.co/Normatividad/LEY%201122%20DE%202007.pdf Consulta: 1 Febrero de 2015]
[72] http://www.minsalud.gov.co/Normatividad/LEY%201438%20DE%202011.pdf [Consulta: 1 Febrero de 2015]
[73] http://www.susalud.com.co[Consulta: 1 Febrero de 2015]

**3.1.2 Reseña histórica.** La institución prestadora de servicios de salud Indígena "Guaitara", nació a la vida jurídica en el año 2005, gracias al interés demostrado por los gobernadores indígenas de los resguardos de Ipiales, San Juan y Yaramal, habilitando los servicios de medicina general, odontología enfermería, servicio farmacéutico, con el objeto social de salvaguardar la salud de la comunidad indígena del municipio de Ipiales, precisamente el día 15 de diciembre de 2005 se obtiene el registro de habilitación número 5235601166 por parte del instituto Departamental de Salud de Nariño, pero, es a partir del primero de abril del año 2005 cuando a través de un contrato de capacitación para cuatro mil quinientos afiliados a la empresa Emssanar, cuando arranca a prestar los servicios de primer.

Para el año 2007, la entidad logró que la eps emssanar, contratara con la institución prestadora de servicios de salud indígena "Guaitara", un total de 6500 afiliados correspondientes en un 90% al resguardo indígena de Ipiales, y en un 10% del resguardo indígena de Yaramal, situación que permitió llegar hasta el 30 de abril del 2008, año en el que la empresa antes mencionada suspende el contrato de capacitación pactada y es a partir del mes de mayo cuando empieza a prestar servicios como epsi Guaitara, atendiendo a 3589 afiliados bajo un contrato de modalidad capitado suscrito hasta el 31 de diciembre de 2008 a la empresa salud Condor eps con 3354 afiliados bajo un contrato de modalidad capitado con vigencia entre 1 de Mayo de 2008 hasta 31 de marzo de 2009.[74]

### 3.1.3 Descripción

- NOMBRE DE LA INSTITUCIÓN: INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA "GUAITARA"
- NIT: 900056747-9[75]
- LOCALIZACIÓN: MUNICIPIO DE IPIALES, DEPARTAMENTO DE NARIÑO.
- CORREO ELECTRÓNICO: ipsiguaitara@gmail.com

La Institución prestadora de servicios de salud indígena "GUAITARA", es una entidad pública de carácter especial sin ánimo de lucro, autorizada y vigilada por la superintendencia nacional de salud, comprometida con la salud, progreso y desarrollo de las comunidades de Ipiales, San Juan y Yaramal.

[74] Tomado de: ANEXO A. Archivo Permanente, Portafolio de Servicios IPSI GUAITARA
[75] http://www.supersalud.gov.co/mapaNarinio.html

La sede principal está ubicada en la avenida panamericana salida al Norte de la ciudad de Ipiales, donde se encuentra el centro de informática encargado de la administración del sistema de información de la empresa; parte de este sistema de información es el servidor que se encarga de la gestión de la base de datos.

Existe una sede satélite a 3 kilómetros, ubicada en carrera 4 N°7-12 Barrio Gólgota en el municipio de Ipiales, esta sede está enlazada a la sede principal por medio de red inalámbrica utilizando dispositivos mikrotik sextant 5hnd que hacen un enlace punto a punto desde la sede principal hasta la sede satélite.

Mikrotik sextant 5hnd son dispositivos que trabajan bajo el estándar inalámbrico 802.11 a/n, trabajan bajo el sistema operativo RouterOS, Las frecuencias están entre los rangos 5.17 a 5.825 GHz y presentan una ganancia de 18dBi que permiten tener una distancia de conexión aproximada de 7 kilómetros sin obstáculos, siendo suficiente para alcanzar la distancia entre los dos puntos de la institución.[76]

**3.1.4 Misión.** Es una entidad prestadora de servicios de salud que garantiza la atención del primer nivel con calidad a toda la población indígena del municipio de Ipiales; orientada a mantener una población saludable; optimizando recursos humanos, económicos y tecnológicos comprometidos con el mejoramiento continuo generando fuentes de trabajo en la región de Ipiales, San Juan y Yaramal [77].

**3.1.5 Visión.** Será una empresa reconocida como una institución líder en su modelo de atención especial para las comunidades indígenas, prestando servicios de salud integral con humanismo, calidad y confianza generada a través de sus trabajadores, usuarios y proveedores[78].

### 3.1.6 Principios corporativos

TRABAJO EN EQUIPO: lo cual nos permite un proceso de capacitación continuo para el mejoramiento de la institución.

SENTIDO DE PERTENENCIA: cuando el personal tiene pertenencia por la institución esto contribuye a prestar servicios con calidad, eficiencia y oportunidad.

[76] DS3, http://www.ds3comunicaciones.com/mikrotik/Sextant%205HnD.html [Consulta: 8 Septiembre de 2015]
[77] Tomado de: ANEXO A. Archivo Permanente, Portafolio de Servicios IPSI GUAITARA
[78] ibíd.

HUMANISMO: permitiendo prestar servicios de acuerdo a las necesidades de nuestras comunidades indígenas.
ÉTICA PROFESIONAL: garantizando el impecable manejo del ejercicio médico y de áreas afines.

EFICIENCIA, EFICACIA Y EFECTIVIDAD: utilizando de manera técnica los recursos para el óptimo logro de los resultados que se ven reflejado en el impacto positivo de nuestras acciones en la salud de la comunidad.

RESPETO: garantizando una atención amable y oportuna de acuerdo a los parámetros de calidad teniendo en cuenta los usos y costumbres de nuestras comunidades indígenas.

LEALTAD: con nuestra misión médica y con la comunidad que requiere de nuestros servicios acogiéndose a la normatividad vigente en nuestra nación[79].

### 3.1.7 Estructura del sistema de información de la IPSI Guaitara.


Figura 1. Estructura del sistema de información. [3]

[79] ibíd.

### 3.1.8 Organigrama

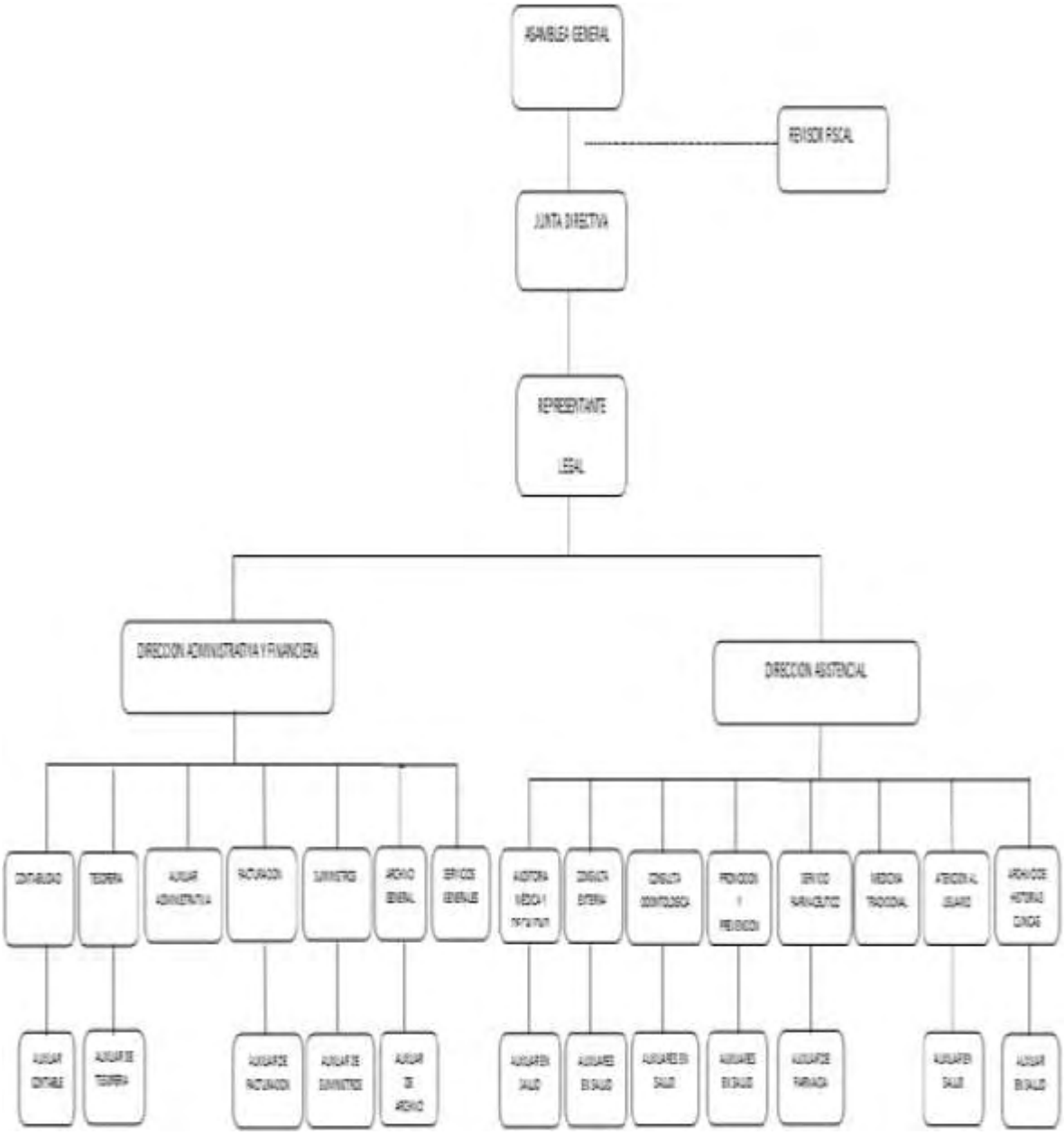



Figura 2. Organigrama IPSI Guaitara. [3]

**3.1.9 Manual de funciones.** Mediante el acuerdo establecido el día 13 diciembre de 2013 se acuerda el "manual específico de funciones y perfiles y competencias laborales de cargos". Manual de funciones de la empresa en donde se detalla los cargos, requisitos, perfiles, experiencia y funciones a desempeñar por los empleados, en el cual se tiene en cuenta el manejo de la información. A continuación, se extrae del acuerdo las funciones correspondientes que se encuentra en el documento digital Manual de Funciones.pdf. en la carpeta:

Evidencias\ANEXO A. Archivo Permanente\Manual de Funciones.pdf.

**FUNCIONES DEL REPRESENTANTE LEGAL**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: directivo
Denominación: representante legal
Nº de cargos: uno (1)
Dependencia: área administrativa
Cargo del jefe inmediato: junta directiva

**II. PROPÓSITO PRINCIPAL**

Dirigir, planear y organizar las políticas y recursos institucionales tendientes a lograr el desarrollo institucional y la atención en salud de la comunidad del área de influencia de la IPS Indígena Guaitara.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Dirigir la IPS Indígena Guaitara, manteniendo la unidad de procedimientos e intereses en torno a la misión y objetivos de la misma.

- Realizar la gestión necesaria para lograr el desarrollo de la IPS. Indígena Guaitara de acuerdo con los planes y programas establecidos del entorno y las condiciones internas de la IPS. Indígena Guaitara.

- Articular el trabajo que realizan los diferentes niveles de la organización, dentro de una concepción participativa de la gestión.

- Ser nominador y ordenador del gasto, de acuerdo con las facultades concedidas por la Ley y los reglamentos.

- Representar a la IPS. Indígena Guaitara judicial y extrajudicialmente.

- Velar por el cumplimiento de las Leyes y reglamentos que rigen la IPS. Indígena Guaitara

- Rendir los informes que le sean solicitados por la Junta Directiva y demás autoridades competentes.

- Presentar los proyectos de acuerdo a través de los cuales se decidan situaciones en la Empresa Social del Estado que deban ser adoptadas o aprobadas por la Junta.

- Celebrar o suscribir los contratos de la IPS. Indígena Guaitara.

- Delegar hasta el nivel directivo las funciones que le han sido encomendadas y las disposiciones legales así lo permitan.

- Presentar a la junta directiva el proyecto de presupuesto de la entidad para la siguiente vigencia fiscal, en el tiempo previsto de acuerdo con las normas legales.

- Participar en el diseño, elaboración y ejecución del plan local de salud, de los proyectos especiales y de los programas de prevención de la enfermedad y promoción de la Salud en coordinación con la alcaldía local y adecuar el trabajo institucional a sus orientaciones.

- Dirigir la elaboración del diagnóstico de la situación de salud del área de influencia de la entidad, interpretar sus resultados y definir los planes, programas, proyectos y estrategias.

- Distribuir los empleados de la Planta Global de la entidad de acuerdo con la naturaleza y responsabilidades.

- Formular las políticas, planes y programas relacionados con la administración y desarrollo del talento humano, los recursos físicos y financieros y recuperación de cartera de la entidad.

- Ejercer la organización, funcionamiento y atención de los servicios asistenciales.

- Ejercer el desarrollo de los procesos de concursos de mérito y demás formas de adquisición de bienes y/o venta de servicios para la entidad, con sujeción a las normas legales vigentes, tanto de derecho privado como Público.

- Dirigir la elaboración del plan de desarrollo científico y tecnológico de la entidad.

- Establecer mecanismos que permitan evaluar y controlar la atención oportuna de las solicitudes formuladas por la ciudadanía y los funcionarios de la Entidad.

- Definir las políticas para el establecimiento y desarrollo de los servicios y procesos internos de planeación, sistemas de información y asesoría jurídica.

- Definir las políticas que se han de seguir para el establecimiento y desarrollo de los sistemas de control interno, de gestión pública y autocontrol y de garantía de la calidad, del sistema de quejas y reclamos y atención al usuario y controlar su funcionamiento.

- Presentar proyectos de inversión ante organismos públicos o privados, nacionales o internacionales, que le permitan mejorar la capacidad operativa en la presentación de servicios de salud.

- Propiciar la aplicación de indicadores de gestión, estándares de desempeño y mecanismos de evaluación y control a cargo de la Entidad.

- Ejercer el control interno sobre las funciones propias del cargo.

- Conocer y fallar en segunda instancia las investigaciones disciplinarias que se siga a los servidores de la entidad con base en lo establecido en el Código Único disciplinario (Ley 734 de 2002) y las demás normas que lo reglamenten, modifiquen o adicionen.

- Responder por el establecimiento y desarrollo del Sistema de Control Interno, estableciendo formalmente un sistema de evaluación y control de gestión, según las características de la Institución y de acuerdo con lo establecido en el Art. 343 de la Constitución Nacional, y en los Art. 6o y 8o de la Ley 87 de 1.993.

- Cumplir y hacer cumplir las normas tendientes a preservar la moralidad de la administración pública de conformidad a lo establecido en la Ley 190 de 1.995.

- Garantizar un sistema técnico de administración de personal que tenga por objeto la eficiencia de la administración pública, la capacitación, la estabilidad en los empleos y el ascenso con base en el mérito, de conformidad en lo establecido en la ley 909 de 2004.

- Evaluar el desarrollo del sistema de control interno relacionado con su área.

- Actualizar los procesos y procedimientos inherentes a su cargo.

- Aplicar el Control Interno sobre las funciones propias del cargo.

- Realizar la segregación y/o clasificación de los desechos peligrosos y no peligrosos en cumplimiento a la normatividad vigente, para la gestión integral de los residuos hospitalarios y similares en Colombia.

- Desempeñar las demás funciones relacionadas con la naturaleza de su empleo y área de desempeño[80].

**FUNCIONES DEL DIRECTOR ADMINISTRATIVO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: directivo
Denominación: director administrativo
Nº de cargos: uno (1)
Dependencia: dirección administrativa
Cargo del jefe inmediato: representante legal IPS. Indígena Guaitara

**II. PROPÓSITO PRINCIPAL**

Implementar las políticas y disponer los recursos institucionales tendientes a lograr el desarrollo institucional y la atención en salud de la comunidad del área de influencia de la entidad.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Planear la prestación de los servicios administrativos y financieros en la IPS Indígena Guaitara.

- Asesorar a la gerencia en la toma de decisiones mediante el análisis financiero y la información oportuna del comportamiento de los ingresos y gastos de la entidad.

- Asesorar la implementación de un sistema de información en red para todos los puntos de atención que conforman la IPS Indígena Guaitara.

[80] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 7 de 71

- Ejercer un control para el cumplimiento del reglamento interno de trabajo, los estatutos, y políticas aprobados por la Junta Directiva, en las áreas de la entidad.

- Coordinar las relaciones de coordinación intra e interinstitucionales necesarias para la adecuada prestación de los servicios administrativos y financieros.

- Ejercer control en la elaboración, actualización y difusión de los manuales de normas y procedimientos de cada una de las áreas.

- Organizar los procesos encaminados a la vigilancia, aseo, mantenimiento de los diferentes puntos de atención de la entidad.

- Participar en el desarrollo de los procesos de Talento humano al interior de la entidad.

- Asesorar a la Gerencia y a las diferentes áreas en el proceso de evaluación del desempeño.

- Presentar oportunamente las respuestas a los entes de control que asi lo requieran.

- Llevar a cabo el control interno sobre las funciones propias de su empleo.

- Ejercer las demás tareas que le sean asignadas y sean afines con la naturaleza del empleo.

- Verificar el desarrollo del sistema de control interno relacionado con su área.

- Actualizar los procesos y procedimientos inherentes a su cargo.

- Aplicar el control interno sobre las funciones propias de su cargo.

- Realizar la segregación y/o clasificación de los desechos peligrosos y no peligrosos en cumplimiento a la Normativa vigente.

- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[81].

[81] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 14 de 71

## FUNCIONES DE TESORERO

## I. IDENTIFICACIÓN DEL CARGO

Nivel jerárquico: profesional
Denominación: tesorero
Nº de cargos: uno (1)
Dependencia: dirección administrativa
Cargo del jefe inmediato: quien ejerza supervisión directa

## II. PROPÓSITO PRINCIPAL

Ejecución de labores profesionales y técnicas relacionadas con el manejo financiero de la IPS. Indígena Guaitara.

## III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

- Recibir fondos de entidades oficiales o de particulares, consignarlos en las cuentas de la entidad y responder por su custodia, así como de valores o dineros encomendados a la dependencia.

- Elaborar la programación de pago de cuentas de cobro, nóminas y planillas de personal, efectuando los respectivos descuentos.

- Responder por el manejo de los fondos, valores, documentos y títulos de propiedad de la empresa y llevar los registros correspondientes, mantener un control estricto de los compromisos adquiridos por la IPS Indígena Guaitara, teniendo en cuenta los vencimientos.

- Elaborar y presentar los informes diarios sobre el movimiento de tesorería, bancos, caja y llevar los libros auxiliares de contabilidad y la relación de bancos de la institución.

- Elaborar y firmar cheques, realizar los procedimientos en las cuentas de cobro de acuerdo con las normas y procedimientos establecidos[82].

## FUNCIONES DE CONTADOR PÚBLICO

## I. IDENTIFICACIÓN DEL CARGO

Nivel jerárquico: profesional
Denominación: contador público

[82] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 18 de 71

Nº de cargos: uno (1)
Dependencia: dirección administrativa
Cargo del jefe inmediato: quien ejerza supervisión directa

## II. PROPÓSITO PRINCIPAL

Liderar el control y análisis de la información financiera, contable, tributaria y presupuestal, garantizando el análisis de la información presentada para realizar un adecuado y oportuno manejo de recursos asignados a la entidad, mediante el desarrollo eficiente de los procesos y procedimientos presupuestales aplicando la normatividad vigente en cumplimiento.

## III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

- Apoyar a la Dirección Administrativa en la toma de decisiones mediante el análisis financiero y la información oportuna del comportamiento de los ingresos y gastos de la Empresa.

- Desarrollar las actividades y procedimientos relacionados con la administración de recursos financieros.

- Proponer a la Dirección Administrativa la aplicabilidad de aspectos administrativos, técnicos, actualización y verificación de normas métodos y procedimientos.

- Elaborar y entregar la información presupuestal, contable y financiera al superior inmediato para su posterior presentación a los órganos de control.

- Preparar y desarrollar los indicadores de gestión propios del área Financiera, y remitirlos con su respectivo análisis a la Dirección Administrativa.

- Coordinar el trabajo del Grupo Funcional mediante mecanismos que garanticen el cabal cumplimiento de los objetivos y metas propuestas en el plan de acción de su dependencia, articulados al plan de desarrollo de la entidad.

- Verificar la gestión del grupo funcional y presentar los informes correspondientes.

- Actualizar los procesos y procedimientos inherentes a su cargo

- Aplicar el control interno sobre las funciones propias de su cargo.

- Realizar la segregación y/o clasificación de los desechos peligrosos y no en cumplimiento a la Normatividad vigente.

- Coordinar de acuerdo a la reglamentación interna de la entidad, el área de desempeño, cuando sea asignado para tal fin.

- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[83].

**FUNCIONES DE PROFESIONAL UNIVERSITARIO DE SISTEMAS DE INFORMACIÓN**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: profesional
Denominación: profesional universitario de sistemas de información
Nº de cargos: Uno (1)
Dependencia: dirección Administrativa
Cargo del jefe inmediato: quien ejerza supervisión directa

**II. PROPÓSITO PRINCIPAL**

Ejecución de labores profesionales de apoyo técnico y administrativo en la aplicación de la información, funcionamiento y administración del sistema de información y computación.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Obtener información útil, oportuna, confiable y económica para responder de forma adecuada a los cambios intra y extra institucionales que generen la demanda de los servicios.

- Implementar, desarrollar, evaluar y retroalimentar el sistema de información de la IPS. Indígena Guaitara.

- Elaborar las normas, procesos y procedimientos para la adquisición y tratamiento del a información de acuerdo con la necesidad de los usuarios.

- Establecer normas y procedimientos para la recuperación, organización, retroalimentación y difusión de la información.

[83] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 20 de 71

- Control, evaluación verificación y observación de las actividades efectuadas en las etapas de captura, registro, transcripción, consolidación, emisión para la generación de la información y aplicación de medidas correctivas cuando los resultados no sean los esperados, la determinación de la satisfacción de los usuarios con relación a la calidad y oportunidad de respuesta a su requerimiento.

- Diseño y elaboración del plan del sistema de información que incluye el plan informático de la IPS Indígena Guaitara.

- Soporte de las demás oficinas de la IPS Indígena Guaitara.

- Mantenimiento de la Red y equipos de cómputo.

- Realización de copias de seguridad de la información.

- Mantenimiento del servidor.

- Reporte a sismed-4505 y demás reportes concordantes[84].

**FUNCIONES DE AUXILIAR ADMINISTRATIVO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel Jerárquico: Asistencial
Denominación: Auxiliar Administrativo (Archivo Historias Clinicas)
Nº de cargos: Uno (1)
Dependencia: Dirección Administrativa
Cargo del Jefe Inmediato: Quien ejerza supervisión directa

**II. PROPÓSITO PRINCIPAL**

Liderar los procesos relacionados con la administración del archivo clínico de la IPS. Indígena Guaitara, siempre en busca de la mejora continua de estos procesos.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Asignar número de historia clínica a los usuarios.

- Mantener actualizadas y organizadas las historias clínicas de cada uno de los servicios.

[84] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 22 de 71

- Entregar historias clínicas solicitadas por los servicios en el orden y en el tiempo solicitado.

- Suministrar las historias clínicas que sean solicitadas para auditorías por los entes competentes

- Procurar la consecución oportuna de los recursos a su cargo y la racional utilización de los disponibles.
- Colaborar en la labores de obtención de información básica de utilidad para el desarrollo de las actividades.

- Promover la interacción entre el servicio de archivo clínico, estadística y el cuerpo médico y enfermería, como así también los demás servicios de la empresa.

- Recibir al usuario e informarle los trámites necesarios para la atención para la entidad y los servicios de esta.

- Recibir, distribuir, actualizar y archivar las historias clínicas y tarjetas que manejan, siguiendo el procedimiento establecido y notificar las inconsistencias que se le presente.

- Archivar exámenes de laboratorio y otros en la respectiva historia clínica.

- Archivar, retirar y llevar del archivo las historias clínicas para los servicios de la empresa.

- Mantener un rígido control sobre el movimiento de las historias clínicas y realizar un informe mensual sobre el control de las mismas.

- Implementar adecuadamente el Archivo de su dependencia según la Ley General de Archivo (594 de 2004).

- Elaborar los informes que sean requeridos por los diferentes entes de control en las fechas estipuladas referentes a información que es generada desde este puesto de trabajo.

- Implementar la cultura del autocontrol en cada una de sus funciones y responsabilidades.

- Desarrollar todos los pasos del proceso y procedimientos de su competencia.

- Desempeñar las demás funciones asignadas por la autoridad competente, las que reciba por delegación y aquellas inherentes a las que desarrolla la dependencia a la profesión del titular del cargo[85].

**FUNCIONES DE AUXILIAR ADMINISTRATIVO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: técnico
Denominación: facturador
Nº de cargos: uno (1)
Dependencia: dirección administrativa
Cargo del jefe inmediato: quien ejerza supervisión directa

**II. PROPÓSITO PRINCIPAL**

Recauda las tarifas por prestación de servicios de salud que se prestan en la IPS. Indígena Guaitara, en lo correspondiente con facturación y cobro de servicios de salud.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Elaborar y digitar la información, documentación y correspondencia de la IPS Indígena Guaitara, en lo correspondiente con facturación y cobro de servicios de salud.

- Recibir, revisar y radicar la correspondencia que llega la IPS con respecto al recaudo, mantenimiento oportunamente informado al Representante Legal.

- Facturar el cobro de Prestación de servicios de salud que presta la IPS

- Indígena Guaitara, conforme a los lineamientos impartidos por la dirección.

- Liquidación de las tarifas adecuadas a las reglamentadas.

- Organizar la información del recaudo para archivo y autoridades competentes.

- Realizar las consignaciones de los recaudos.

[85] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 22 de 71

- Organizar técnicamente el archivo de la correspondencia enviada y recibida, de documentos importantes y de los expedientes que el Tesorero crea conveniente abrir, mantenerlo actualizado, dejando copia de toda remisión en dicho archivo.

- Llevar y conservar estrictamente el orden consecutivo de la correspondencia originada en la tesorería.

- Colaborar en la organización técnica y de apoyo para el buen funcionamiento del archivo institucional.

- Controlar y relacionar en la planilla de control, los recaudos de la IPS de las obligaciones propias de la entidad.
- Guardar la debida reserva de los documentos y asuntos que se traten en la tesorería.

- Atender al público suministrando la información pertinente y resolviendo, si es del caso, asuntos que sean de su competencia.
- Velar por el buen uso y mantenimiento de los equipos a su cargo.

- Cumplir las demás funciones que le sean asignadas en razón de su cargo para beneficio de las labores generales de la Entidad[86].

**FUNCIONES DE DIRECTOR ADMINISTRATIVO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: directivo
Denominación: director asistencial
Nº de cargos: uno (1)
Dependencia: dirección asistencial
Cargo del jefe inmediato: representante legal IPS Indígena Guaitara

**II. PROPÓSITO PRINCIPAL**

Ejecutar labores de dirección, asesoría, supervisión y control de los planes de salud, programas y normas técnicas a fin de garantizar la prestación de servicios de salud a la comunidad.

[86] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 22 de 71

## III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

- Orientar alternativas estratégicas para el desarrollo de los servicios y alcanzar mayores niveles de cobertura Institucional.

- Dirigir las políticas de salud formuladas, así mismo, colaborar con las mediciones de impacto respectivas.

- Ejercer control y seguimiento integrando las diferentes áreas para garantizar la calidad del servicio.

- Coordinar los procesos de evaluación de la calidad en el servicio.

- Prever la consecución oportuna de los recursos necesarios para la correcta prestación del servicio, promover la utilización racional de los disponibles con criterios de calidad, eficiencia, productividad.

- Asesorar a la Dirección en la determinación e implementación de políticas, estrategias, planes y programas en materia de planificación, distribución y desarrollo de los servicios de salud.

- Realizar el plan de adquisiciones y suministros, de acuerdo con las normas vigentes para la institución.

- Brindar apoyo logístico para el desarrollo de los planes, programas y proyectos aprobados en la IPS Indígena Guaitara.

- Verificar el desarrollo del sistema de control interno relacionado con su área.

- Actualizar los procesos y procedimientos inherentes a su cargo

- Aplicar el control interno sobre las funciones propias de su cargo

- Realizar la segregación y/o clasificación de los desechos peligrosos y no en cumplimiento a la Normatividad vigente.

- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[87].

[87] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 40 de 71

## FUNCIONES DE MÉDICO GENERAL

## I. IDENTIFICACIÓN DEL CARGO

Nivel jerárquico: profesional
Denominación: médico general
Nº de cargos: siete (7)
Dependencia: dirección asistencial
Cargo del jefe inmediato: quien ejerza la supervisión directa

## II. PROPÓSITO PRINCIPAL

Dirigir la dirección inicial del paciente en el área correspondiente comenzando por la valoración, diagnóstico y clasificación de la complejidad de la patología, reconoce si requiere o no la atención en este servicio; ofrece su capacidad médico-científica, ética y humana para la recuperación del buen estilo de salud del paciente.

## III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

- Practicar exámenes de medicina general, establecer diagnóstico y prescribir el tratamiento.

- Realizar historias clínicas, completas con motivo de consulta, enfermedad actual, examen físico completo, diagnóstico, tratamiento, recomendaciones y evolución, así como las Epicrisis.

- Realizar las acciones de salud pública de su responsabilidad en la promoción de la salud, prevención de la enfermedad, tratamiento y rehabilitación necesarios en los diferentes grupos del ciclo evolutivo y de acuerdo con la normatividad vigente.

- Apoyar el desarrollo de estrategias de participación social con los diferentes actores locales con el fin de garantizar la pertinencia y efectividad de las intervenciones e impulsar y motivar la conformación de grupos de participación social.

- Participar en la elaboración y actualización del diagnóstico de salud del área de influencia de la IPS Indígena Guaitara.

- Evaluar junto con el equipo de salud, la eficiencia y el impacto de los programas ofrecidos a la comunidad

- Realizar la referencia y contra referencia cuando se requiera, dentro de la estrategia de redes de servicios de salud y de acuerdo con las normas que la regulan.

- Participar en las acciones de vigilancia epidemiológica para situaciones que sean factor de riesgo para la población.

- Identificar necesidades y participar en estudios tendientes a solucionar problemas de salud de la comunidad.

- Propiciar las relaciones de coordinación necesarias para lograr una eficaz prestación de los servicios de salud.

- Participar en el análisis de la información de oferta y demanda de servicios de salud del área de influencia que permita proponer alternativas de solución.

- Diligenciar de manera clara, completa y oportuna, los instrumentos que le sean encomendados para el ejercicio de su actividad.

- Aplicar las normas, guías y protocolos que garanticen la adecuada prestación del servicio.

- Participar en la actualización del manual de normas y procedimientos de su área.

- Reportar oportunamente las anomalías en la prestación del servicio

- Presentar informe periódicos sobre el desarrollo de las funciones

- Verificar el desarrollo del sistema de control interno relacionado con su área.

- Actualizar los procesos y procedimientos inherentes a su cargo.

- Aplicar el control interno sobre las funciones propias de su cargo

- Realizar la segregación y/o clasificación de los desechos peligrosos y no en cumplimiento a la Normatividad vigente.

- Coordinar de acuerdo a la reglamentación interna de la entidad, el área de desempeño, cuando sea asignado para tal fin.

- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[88].

**FUNCIONES DE PSICÓLOGO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: profesional
Denominación: psicólogo(a)
Nº de cargos: uno (1)
Dependencia: dirección asistencial
Cargo del jefe inmediato: quien ejerza la supervisión directa

**II. PROPÓSITO PRINCIPAL**

Promover y contribuir al mejoramiento de la salud mental de los usuarios de la entidad mediante intervención terapéutica con un enfoque integral e interdisciplinario dentro del marco legal, ético y científico con calidad eficiencia y oportunidad.

**III. DESCRIPCIÓN DE FUNCIONES ESENCIALES**

- Ejercer funciones de tipo asistencial a toda persona o grupo que requiera los servicios psicológicos de prevención, diagnóstico, tratamiento y rehabilitación.

- Aportar elementos válidos y confiables que permitan la valoración integral de las personas que solicitan el servicio mediante la historia clínica y técnicas específicas para su diagnóstico y definición de la conducta a seguir.

- Realizar intervención psicoterapéutica a nivel individual, familiar y grupal que permitan el logro de los objetivos terapéuticos establecidos a partir de la valoración y diagnóstico para contribuir a los procesos de rehabilitación y calidad de vida que la regulan.

- Realizar la referencia y contra referencia cuando se requiera, dentro de la estrategia de redes de servicios y de acuerdo a las normas que la regulan.

- Participar en las acciones en vigilancia epidemiológica para situaciones que sean factor de riesgo para la población.

[88] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 40 de 71

- Apoyar diferentes programas para prevención y atención de violencia intrafamiliar, abuso sexual y situación de crisis.

- Participar en las actividades de la red de Salud Mental con el fin de revisar y actualizar políticas de salud mental y el cumplimiento del plan de acción acorde con dichas políticas.

- Diligenciar de manera clara, completa y oportuna, los instrumentos que le sean encomendados para el ejercicio de su actividad.

- Aplicar las normas, guías y protocolos que garanticen la adecuada prestación del servicio.

- Participar en la actualización del manual de normas y procedimientos de su área.

- Realizar control interno sobre las funciones propias de su cargo.

- Coordinar de acuerdo a la reglamentación interna de la entidad, el área de desempeño, cuando sea asignado para tal fin.
- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[89].

**FUNCIONES DE BACTERIÓLOGO**

**I. IDENTIFICACIÓN DEL CARGO**

Nivel jerárquico: profesional
Denominación: bacteriólogo
Nº de cargos: uno (1)
Dependencia: dirección asistencial
Cargo del jefe inmediato: quien ejerza la supervisión directa

**II. PROPÓSITO PRINCIPAL**

Tomar y procesar muestras de los exámenes de genética solicitados cumpliendo con los estándares de calidad establecidos para responder los requerimientos de diagnóstico y tratamiento de los usuarios contando con la tecnología adecuada y el recurso humano calificado y competente.

[89] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 45 de 71

## III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

- Realizar los análisis de las diferentes áreas que integran el laboratorio de bacteriología en forma oportuna y confiable con ética y responsabilidad para emitir los resultados requeridos por los usuarios.

- Elaborar pruebas de control de calidad de los análisis clínicos realizando la verificación de la calibración de cada uno de los instrumentos cuando corresponda, según cronograma con el fin de garantizar la veracidad de los resultados.

- Tomar las muestras con los conocimientos necesarios en forma adecuada y seguirá siguiendo los parámetros establecidos dando la seguridad y confianza al paciente para obtener una muestra óptima y confiable.

- Orientar e informar a los pacientes sobre los requisitos para la toma de una muestra y sobre la forma de recolección de las mismas.

- Preparar y controlar los reactivos, las sustancias de referencia, soluciones y los medios de cultivos necesarios en el laboratorio y responder por el adecuado uso de los equipos y elementos asignados emitiendo los conceptos requeridos para su adquisición.

- Supervisar los procedimientos de la toma de muestras, coloración, montaje y lavado de material.

- Correlacionar los resultados obtenidos en forma oportuna y confiable con la historia clínica del paciente para responder a los requerimientos necesarios para emitir un posterior diagnóstico y tratamiento.

- Aplicar las normas, guías y protocolos que garanticen la adecuada prestación del servicio.

- Participar en la actualización del manual de procesos y procedimientos del área.

- Reportar oportunamente las anomalías en la prestación del servicio

- Presentar informe periódicos sobre el desarrollo de las funciones

- Capacitación continua, en las diferentes áreas del laboratorio con apoyo de la institución para el crecimiento personal e institucional.

- Verificar el desarrollo del sistema de control interno relacionado con su área.

- Actualizar los procesos y procedimientos inherentes a su cargo

- Aplicar el control interno sobre las funciones propias de su cargo

- Realizar la segregación y/o clasificación de los desechos peligrosos y no en cumplimiento a la Normatividad vigente.

- Desempeñar las demás funciones relacionadas con la naturaleza del empleo y área de desempeño[90].

### 3.1.10 Reconocimiento del software de apoyo INFO-SALUD en la institución

Teniendo en cuenta que la IPSI GUAITARA requiere dar cumplimiento a la Resolución 4505 de 2012[91] que ordena a las IPS disponer de un medio tecnológico que permita generar la información de atención a pacientes de manera correcta y oportuna, la cual se debe reportar al Ministerio de Salud y Protección Social, y así optimizar recursos y lograr mejores resultados en el cumplimiento de metas de gestión.

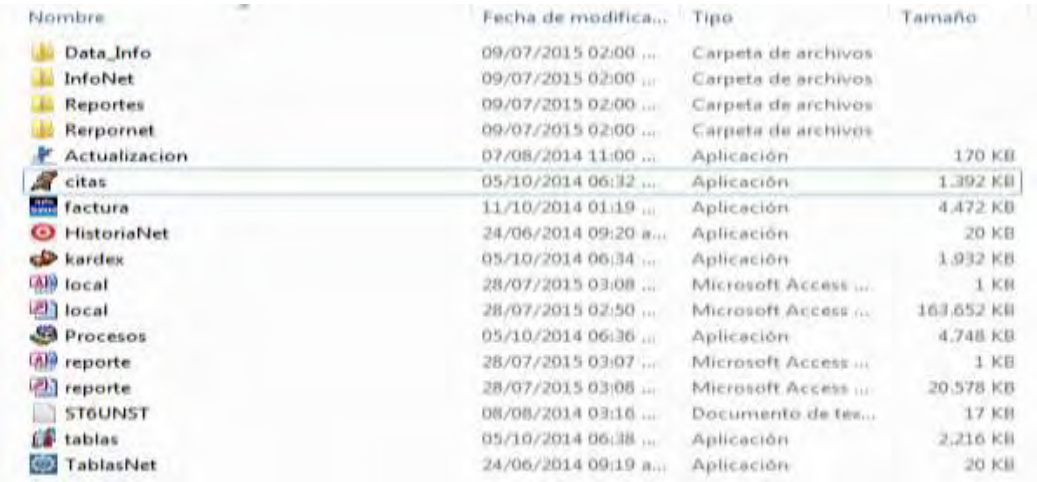



Figura 3. Vista general módulos INFO-SALUD. [1]

[90] Anexo MANUAL DE FUNCIONES IPSI GUAITARA pág. 47 de 71

[91] MINSALUD,http://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%204505%20de%202012.pdf

**a) Módulo de citas médicas**


Figura 4. Pantalla de ingreso al módulo de citas médicas. [1]

Este módulo cumple con el objetivo de organizar el proceso mismo de consulta, se encarga de la planeación de la agenda médica programando equitativamente el tiempo y el recurso médico para garantizar la mejor atención al paciente.

Los operarios encargados de manejar este módulo ingresan en la aplicación la información personal de cada paciente y horario disponible para la asignación de las citas médicas[92].

Actualmente el módulo de citas médicas realiza los siguientes procesos:

- **Creación de agenda médica**

  El módulo muestra en pantalla un calendario correspondiente al mes y año, una especialidad y un profesional.

  Se procede a seleccionar la especialidad y el médico para luego programar una agenda médica para cada profesional escogiendo semana, día y hora para asignar citas con intervalos de tiempo estipulados.

[92] Fuente: Investigación de este trabajo

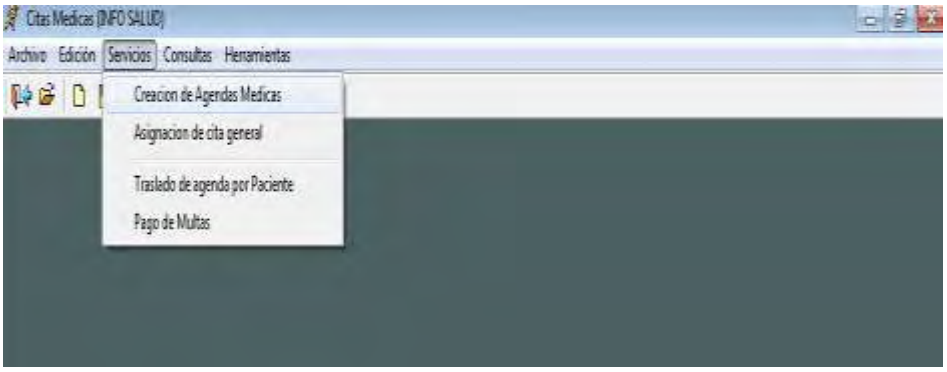



Figura 5. Pantalla principal módulo de agenda médica. [1]

- **Asignación, cancelación o reprogramación de citas**

  Este proceso empieza cuando el paciente se acerca a la IPSI GUAITARA a solicitar una cita, allí el operario revisa la agenda del profesional de la salud y registra en el sistema los datos del paciente y asigna un día y una hora para cita.

  De este proceso hacen parte la cancelación y reprogramación de citas; de igual manera el usuario se acerca a las instalaciones de la IPSI y solicita la cancelación o reprogramación de su cita médica, el operario realiza una búsqueda de citas médicas ingresando el número de identificación del usuario y se procede a la cancelación o cambio de fecha de la cita correspondiente.

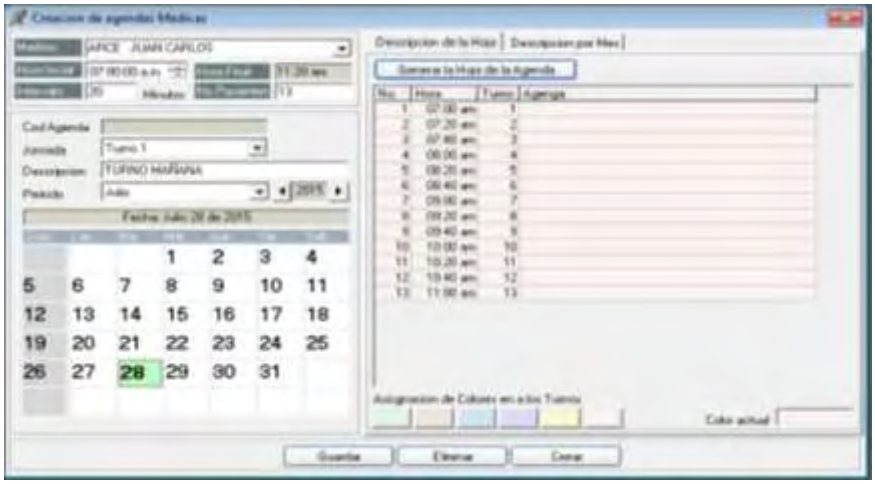


Figura 6. Creación de agenda médica. [1]

- **Verificación de datos**

  El sistema valida la información ingresado por el operario de asignación de citas y si está correcta se procede a escoger el día y hora de la cita a solicitar.

  Para el correcto funcionamiento de este proceso, el usuario debe estar registrado en la base de datos de usuarios de la entidad, de lo contrario no se puede solicitar la cita médica.

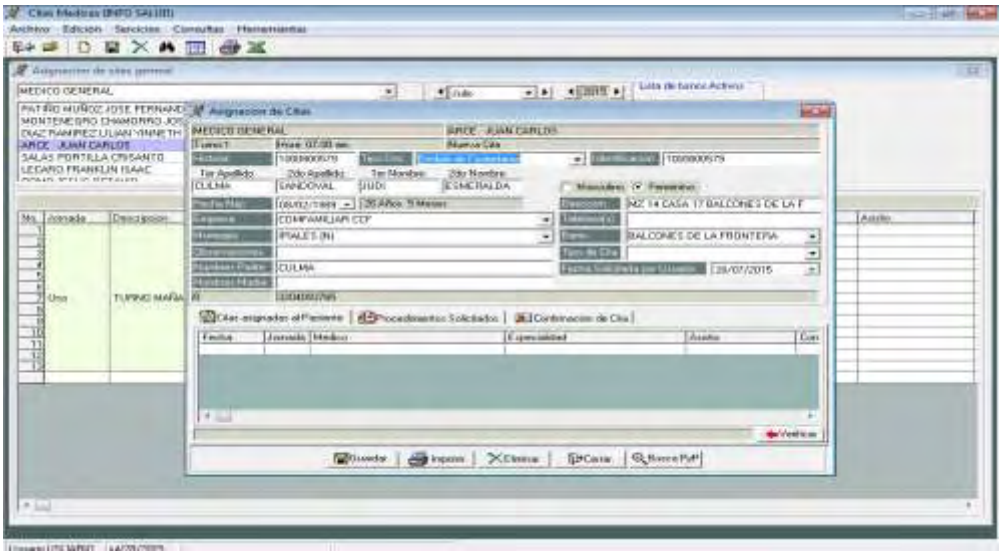


Figura 7. Asignación de cita. [1]

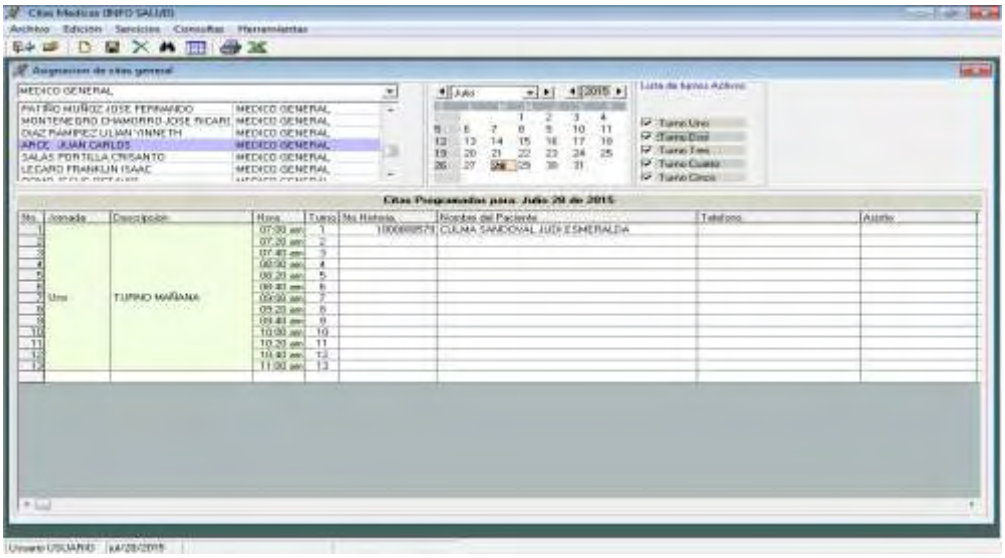


Figura 8. Asignación de fecha y hora de cita. [1]

- **Aplicar multas por inasistencia**

  El sistema lleva registros de incumplimientos de citas médicas las cuales conllevan a multas por parte de la IPSI por el incumplimiento conforme lo previsto en el artículo 55 de la Ley 1438 de 2011[93].

  El sistema permite registrar el pago de multas por parte de los usuarios que por motivos personales no pudieron cumplir con la asistencia a la cita médica.

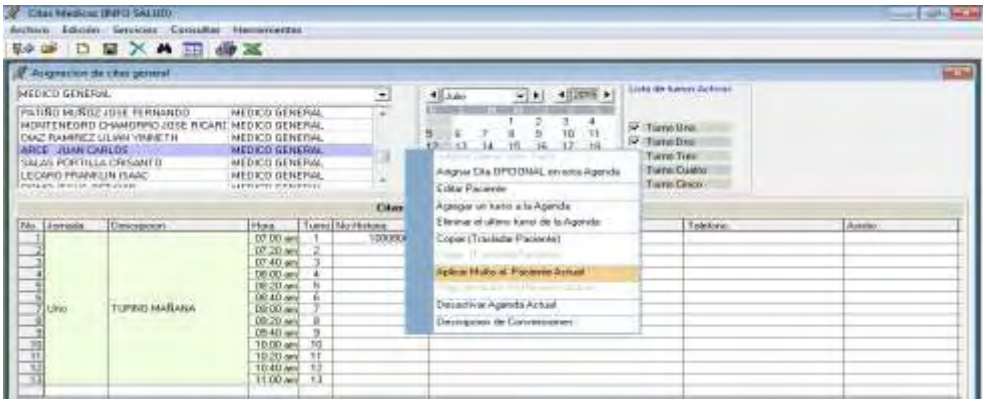


Figura 9. Aplicar multas por inasistencia. [1]

❖ **Características generales**

- Creación de agenda médica (mensual, semanal y diario).
- Asignación de los turnos (citas de control, primera vez o pyp).
- Registro de la actividad de los usuarios.
- Funcionamiento del control calendario.(no hay festivos en el calendario)
- Generación de listados de agendas médicas.
- Búsqueda de turnos asignados.
- Definición de tabla de horarios.

[93] MINISTERIO DE SALUD, ley 1438,2011, ttps://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/LEY%201438%20DE%202011.pdf#search=1438[Consulta: 15 de Diciembre de 2014]

- Manejo de estados de citas como cumplimiento, cancelación e incumplimiento.

❖ **Características específicas**

- Permite consultar las agendas programadas de forma diaria, semanal o mensual.

- Permite la reprogramación de citas.

- El programa genera reportes y estadísticas que brindan información sobre los datos capturados en la agenda, como asistencia de pacientes y carga de trabajo de los médicos.

- Citas imprimibles. Las citas de los pacientes se pueden imprimir en vista semanal o diaria para uno o todos los médicos.

- Permite la asignación de citas extras sin que se modifique el horario del profesional de la salud.

- Permite aplicar multas a los usuarios por inasistencia a una cita médica.

- Asignación de colores según el régimen al cual pertenezca el usuario. (contributivo, subsidiado, vinculado, particular, otro)

- Asignación de colores según cupos en la agenda médica (agenda con cupo disponible, agenda con cupo completo).

❖ **Visión general**

A continuación, se muestra mediante un cuadro simplificado de las entradas, salidas y procesos del módulo de citas médicas.

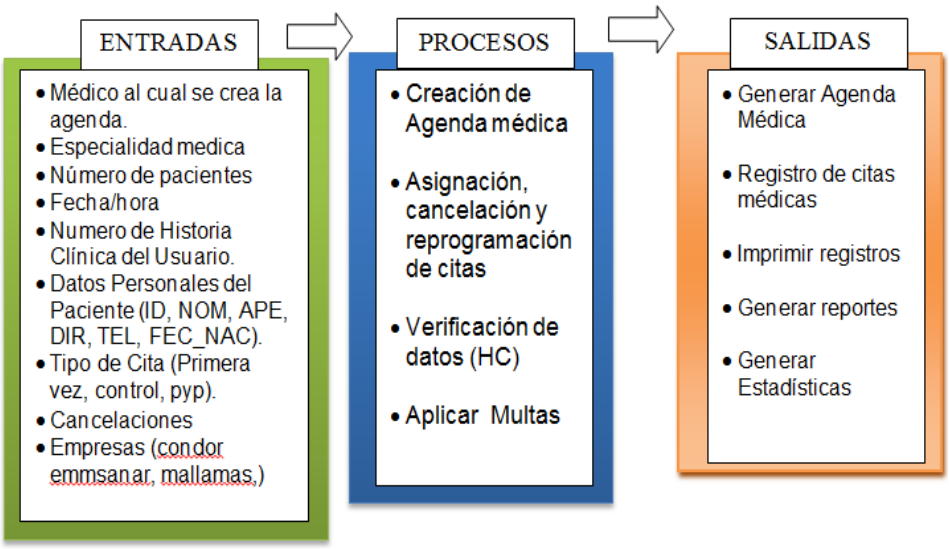



Figura 10. Cuadro funciones de módulo de citas médicas. [1]

**b) Módulo de historia clínica - historianet**

HistoriaNet es el módulo encargado de la administración de las historias clínicas pertenecientes a los usuarios de la IPS Indígena Guaitara.

La historia clínica es el documento que contiene toda la información médica de una persona. Es la fuente básica para la atención al paciente, para la realización de investigaciones, y constituye un apoyo imprescindible en el área médico[94].


Figura 11. Pantalla de ingreso al módulo de historia clínica. [1]

[94] Fuente: Investigación de este trabajo

Este módulo se encarga del registro de manera cronológica el estado de salud del paciente, los actos médicos y demás procedimientos que conllevan a garantizar una atención de calidad al usuario.

Los encargados de manejar este módulo es el personal médico (enfermeras jefes, odontólogos, médicos generales y auxiliares de enfermería encargadas de llevar los registros referentes a post consulta) el cual registra datos en forma cronológica y secuencial de los síntomas del paciente con el fin de entender su problema de salud.

Actualmente el módulo historianet contiene los siguientes sub-módulos:

❖ **Servicios**

El sub módulo servicios permite al profesional de la salud acceder de forma rápida los principales datos de los pacientes por medio de métodos como:

- **Tarjetero**

  Contiene información relacionada con los datos biográficos básicos del usuario (nombre, edad, sexo) y permite que sea consultado todas las veces que sea necesario, por la practicidad que implica y la disponibilidad.

- **Admisión de paciente**

  Permite ingresar el principal motivo de consulta, en este proceso no se lleva a cabo un tratamiento médico especializado, sólo es parte del procedimiento de ingreso.

  Al ser diligenciado este proceso, el médico podrá darse cuenta cual es el principal síntoma de consulta del usuario.

- **Agenda médica**

  Esta opción proporciona al profesional de la salud visualizar los pacientes citados en la actual jornada. La pantalla muestra una lista en la cual se observa turnos, hora, nombre del paciente y los diagnósticos que se han realizado en anteriores consultas.

- **Hospitalización**

  Esta opción permite registrar el tipo de ingreso de un paciente (triage, urgencias, hospitalización), pabellón o sección donde estará el paciente

(ginecología, sala de mujeres, pediatría, traumatología, sala de observación, urgencias), días de estancia y Diagnóstico.

Esta opción está diseñada para un centro de salud de Nivel II, pero en este caso no es utilizada debido a que la IPSI Guaitara es una institución de nivel I.


Figura 12. Submódulo de servicios. [1]

❖ **Registros historia clínica**

Este sub-módulo contiene el proceso de ingresar la historia clínica del paciente, el cual es un documento médico-legal que surge de la relación entre el profesional de la salud y el paciente, tiene como función recoger la información necesaria para la correcta atención de los pacientes. La historia clínica es un documento válido desde el punto de vista clínico y legal, que recoge información de tipo asistencial, preventivo y social.

A este módulo pertenecen los siguientes procesos:

- **H.C**

  Permite ingresar y verificar anteriores sintomatologías, mediante la cual el paciente ha solicitado citas médicas; en este proceso se encontró campos que el profesional de la salud debe ingresar.

  ✓ Enfermedad actual

- ✓ Antecedentes personales
- ✓ Antecedentes obstétricos
- ✓ Antecedentes ginecológicos
- ✓ Antecedentes familiares
- ✓ Revisión por sistema
- ✓ Signos vitales
- ✓ Examen físico
- ✓ Examen mental
- ✓ Intervención médico familiar
- ✓ Diagnóstico (donde existen ayudas para identificar los diferentes códigos médicos para cada enfermedad, si el profesional ingresa una palabra clave de la sintomatología).
- ✓ Recomendaciones
- ✓ Tratamiento
- ✓ Estudio general
- ✓ Notas aclaratorias

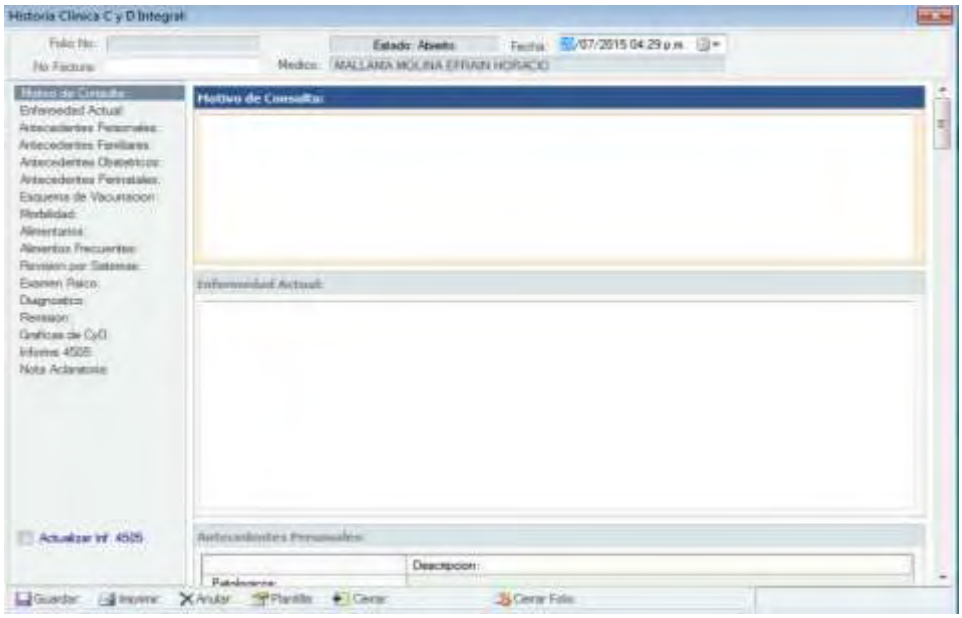



Figura 13. Registro de sintomatología. [1]

En este proceso existen opciones como “no refiere” cuando los datos no son necesarios para la consulta y “todo normal” cuando los signos vitales o exámenes físicos son normales, esto con el fin de brindar mayor agilidad a la hora de ingresar datos del paciente.

- **Evolución**

  Se registra un resumen de la sintomatología del paciente, para dar seguimiento a su progreso. Debe ser precisa y completa que la historia clínica teniendo en cuenta los puntos más importantes de la enfermedad.

- **Notas de enfermería**

  Este proceso permite la valoración al paciente por parte del personal de enfermería, el cual se encargará de verificar los datos personales del paciente, registro de signos vitales y observación de las condiciones físicas generales.

- **Ordenes médicas**

  Esta función permite al profesional de la salud prescribir servicios y/o tratamientos que el paciente necesita. Incluye campos como son orden de procedimientos con su respectivo código, observaciones, orden de texto y configuración de impresión.

- **Fórmula médica**

  La fórmula médica es el documento legal por medio del cual los médicos capacitados prescriben la medicación al paciente para su dispensación por parte del farmacéutico. En este proceso el profesional de la salud ingresa la medicación con su respectivo código y descripción, dosis que considere el médico y observaciones necesarias para la correcta dosificación del medicamento al paciente.

- **Ayudas diagnósticas**

  Existen varios métodos para apoyo al diagnóstico médico entre los cuales INFO-SALUD cuenta con plantillas para la solicitud y verificación de resultados de exámenes de:

  ✓ **Laboratorio clínico:** muestra resultados de parcial de orina, coprológico, química sanguínea, frotis vaginal y hematología.

  ✓ **Imagenología RX**

  ✓ **Notas quirúrgicas**

- **Certificados**

  El software cuenta con formatos para certificados médicos en donde el profesional de salud realiza una declaración que da fe del estado de salud de una persona en un determinado momento.

Entre las plantillas ingresadas en este sub-módulo están:

- Concepto médico
- Incapacidad
- Certificado de trabajo
- Certificado médico ocupacional

❖ **Características generales**

Permite almacenar un historial de tratamientos de pacientes como antecedentes médicos, diagnóstico, radiografías, exámenes y evolución.

Genera un resumen cronológico del historial clínico de un paciente desde antecedentes hasta las recetas emitidas y procedimientos realizados.

Historia clínica electrónica con reportes imprimibles en caso que requiera almacenamiento o revisión física de la información.

Permite almacenar imágenes médicas como radiografías, TACs entre otras.

- Triage urgencias
- Consulta urgencias
- Consulta externa
- Consulta odontológica
- Enfermedades crónica
- Consulta pre anestésica
- Oftalmología
- UCI neonatal
- Historia Cir. vascular
- Pediatría especializada
- Laboral
- Interpretación de ayudas diagnósticas
- Epicrisis
- Salida
- Terapia física
- Psicóloga
    - ✓ Asesoría psicológica postparto
    - ✓ Asesoría psicológica
- Fonoaudiología
- Optometría

- Historia ocupacional
- Consultas PYP
    - ✓ PYP AIDEPI de 2 a 5 años
    - ✓ PYP AIDEPI menor de 2 meses
    - ✓ PYP AIDEPI de 5 a 9 años
    - ✓ PYP AIDEPI escala abreviada de desarrollo
    - ✓ PYP higiene oral
    - ✓ PYP higiene oral 2
    - ✓ PYP adulto mayor
    - ✓ PYP agudeza visual
    - ✓ PYP planificación familiar
    - ✓ PYP índice riesgo reproductivo
    - ✓ PYP alteraciones del joven
    - ✓ PYP citología
    - ✓ PYP materno-perinatal
    - ✓ PYP materno-perinatal control
    - ✓ PYP materno-perinatal parto/aborto

❖ **Visión general**

A continuación, se muestra mediante un cuadro simplificado las entradas, salidas y procesos del módulo de kardex.


Figura 14. Cuadro funciones de módulo historia clínica. [1]

c) **Módulo de facturación**


Figura 15. Pantalla de ingreso al módulo de facturación. [1]

El proceso de facturación son el conjunto de actividades que permiten cuantificar la prestación de los servicios de salud producto de la atención al usuario. La IPS, como cualquier empresa productora de bienes o servicios debe garantizar su mantenimiento mediante la venta de servicios asistenciales. Según la reglamentación del Sistema General de Seguridad Social en Salud (SGSSS) toda IPS debe realizar un registro sistemático e individual de los procedimientos y servicios prestados a cada usuario, liquidarlos a las tarifas establecidas y realizar el cobro a las instancias pertinentes.

El módulo facturación del software INFO-SALUD, permite llevar un control de los medicamentos y servicios ofrecidos a los pacientes, este módulo es utilizado por las áreas de facturación y farmacia de la IPSI Guaitara[95].

La barra del menú principal del módulo se compone de las opciones:

- Archivo
- Edición
- Servicios
- Herramientas
- Reportes

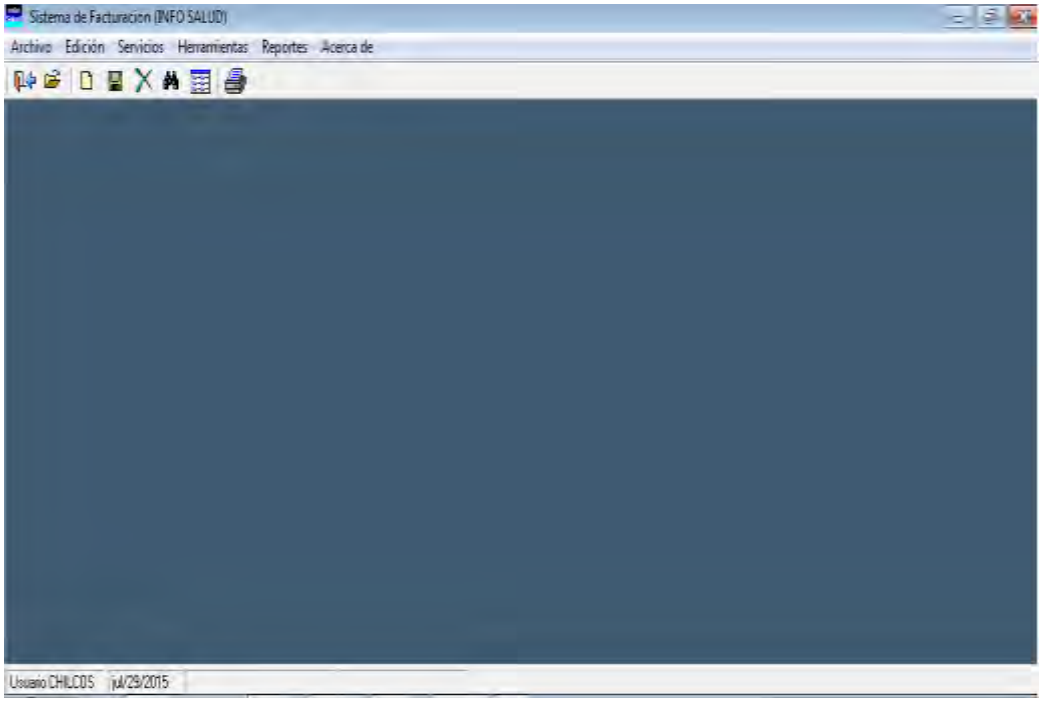



Figura 16. Pantalla principal del módulo de facturación. [1]

La opción más destacada del menú principal es servicios en donde se encuentra las opciones de facturación general. Es la opción más utilizada en la entidad a la hora de hacer el registro de la prestación de un servicio y entrega de un medicamento.

El personal encargado de manejar esta opción debe ingresar en la aplicación el número de historia clínica, esto con el fin de conocer los nombres, apellidos,

[95] Fuente: Investigación de este trabajo

género, fecha de nacimiento, edad, empresa a la que está afiliado, estrato, dirección y demás datos personales de cada paciente.

Posteriormente, se debe ingresar el tipo de contrato, cabe destacar que debido al nivel de complejidad de atención de la empresa (nivel 1), la entidad ofrece los servicios de medicina asistencial (consulta médica general, odontología general) y PyP (promoción y prevención) por ello algunas de las funciones que ofrece este módulo no se utilizan en la IPSI Guaitara.

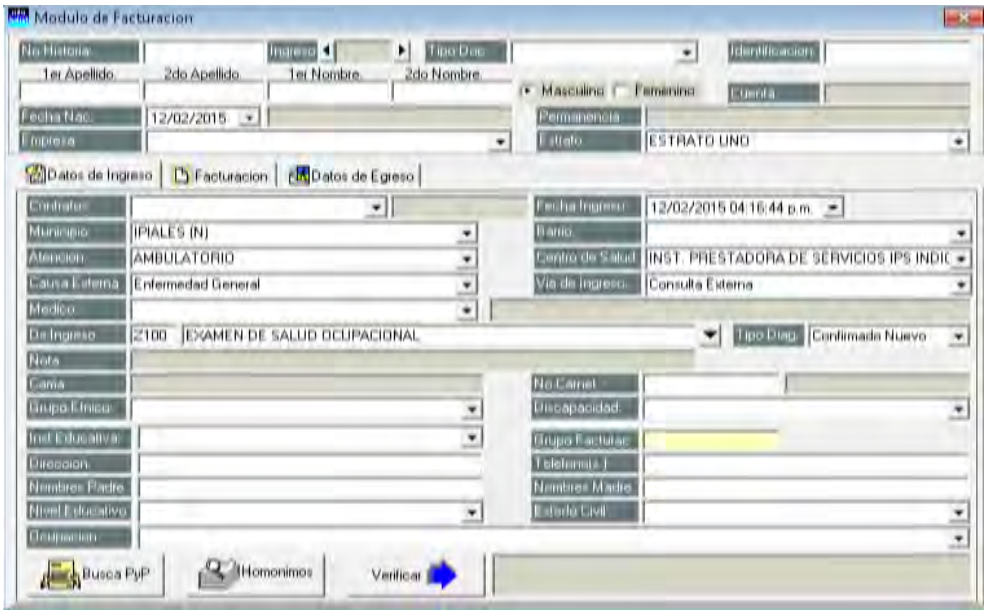


Figura 17. Facturación general. [1]

❖ **Características específicas**

El módulo de facturación es utilizado para generar registros de:

- Facturación de servicios (puede ser PYP ó asistencial)
- Facturación de servicios extramurales
- Facturación de medicamentos

El módulo facturación tiene un sub-módulo llamado procesos, este módulo principalmente hace informes de relación que la entidad necesite para analizar el funcionamiento y generar RIPS (Registro individual de prestación de servicios de salud) conforme la ley lo determina en el decreto 4747 de 2007: Artículo 20 del Ministerio de Protección Social[96].

[96] Tomado de: http://www.minsalud.gov.co/Normatividad/DECRETO%204747%20DE%202007.pdf

- ✓ Reportes de facturación por pacientes
- ✓ Reportes de servicios médicos
- ✓ Controlar la base de datos de afiliados
- ✓ Reportes de facturación puede ser asistencial o PyP
- ✓ Detallado de totales, cantidad, códigos, medicamentos o procedimientos
- ✓ El reporte PyP por actividades mostrando las actividades con su procedimiento y la cantidad total. Permite mirar de forma detallada, qué cantidad ha facturado y que cantidad le falta por facturar.}
- ✓ Número de consultas de medicina general se han hecho en un periodo de tiempo (facturación general)
- ✓ Identificar los pacientes atendidos en las consultas de medicina general (reportes detallados agrupados por parámetros)

Una funcionalidad a destacar, es la posibilidad de exportar a Excel la información ya sea para consultarla o para editar la misma, permitiendo así la corrección o edición.

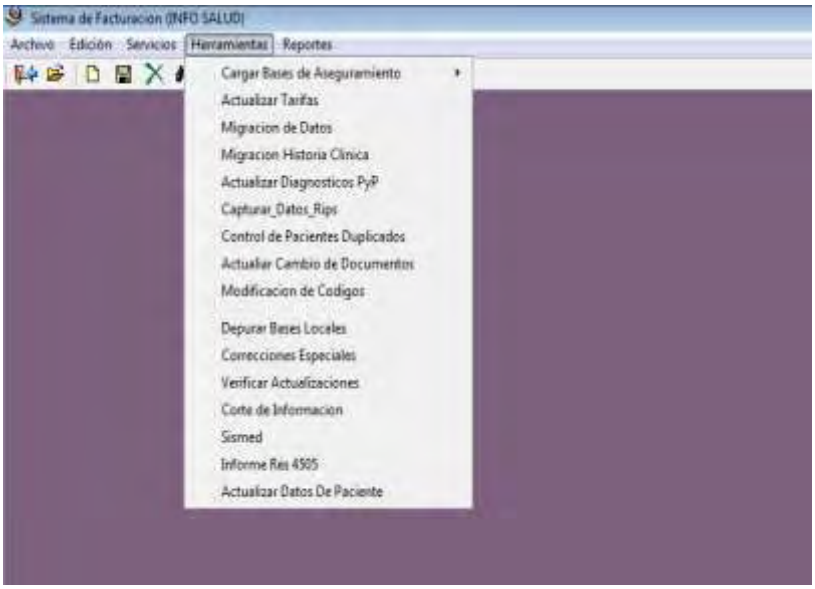



Figura 18. Sub-módulo procesos**.** [1]

### d) Módulo de kardex

El kardex es un registro organizado de la mercancía que se tiene en bodega. Para actualizar los datos, es necesario un inventario de todas las existencias por contenido, cantidad, un valor de medida y precio unitario[97].


Figura 19. Pantalla de ingreso a módulo kardex. [1]

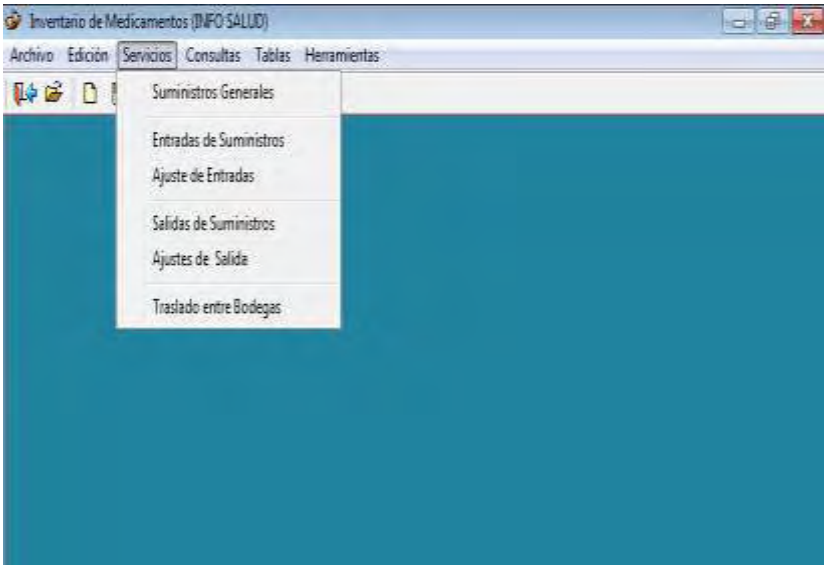



Figura 20. Pantalla principal kardex opción servicios. [1]

El módulo de kardex de INFO-SALUD tiene la opción de administrar y controlar el inventario de medicamentos registrando tanto las entradas como las salidas de

[97] Fuente: Investigación de este trabajo

cada medicamento. Es utilizado principalmente en el área de farmacia para el control de inventarios de medicamentos.

El menú principal presenta las opciones de:

- Archivo
- Edición
- Servicios
- Consultas
- Tablas
- Herramientas

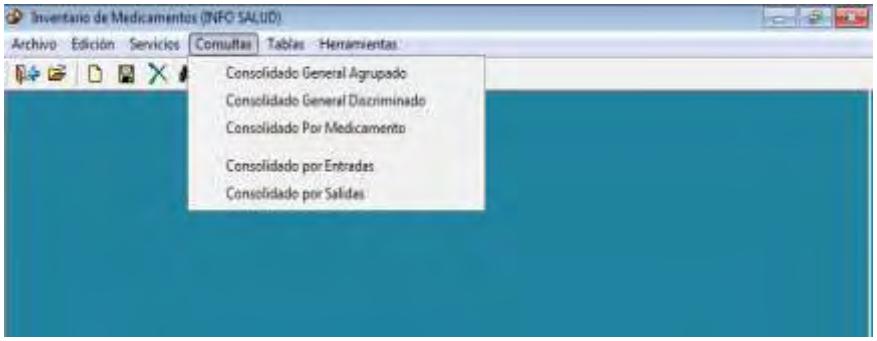



Figura 21. Pantalla principal kardex opción consultas. [1]

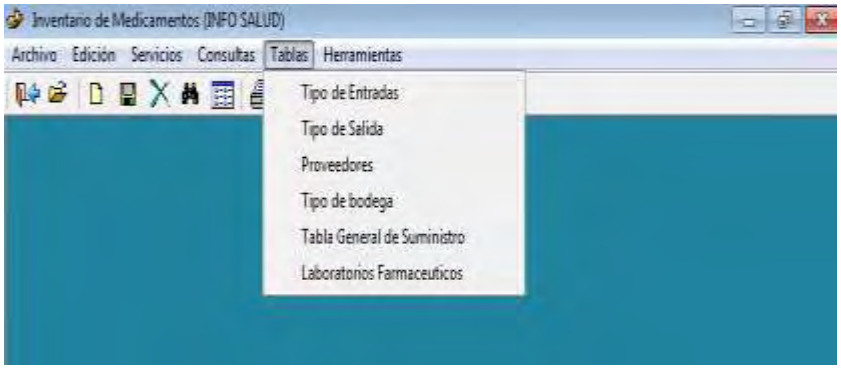



Figura 22. Pantalla principal kardex opción tablas. [1]

Los módulos de facturación y kardex están enlazados de manera que si se hace el registro de una venta en facturación, automáticamente disminuye la cantidad de existencias registradas.

Los procesos manejados en el módulo de kardex, son:

- ✓ Inventario de medicamentos
- ✓ Inventario de insumos
- ✓ Ingreso de medicamentos e insumos
- ✓ Salida de medicamentos e insumos
- ✓ Administración de bodegas

A continuación, se muestra mediante un cuadro simplificado las entradas, salidas y procesos del módulo de kardex.

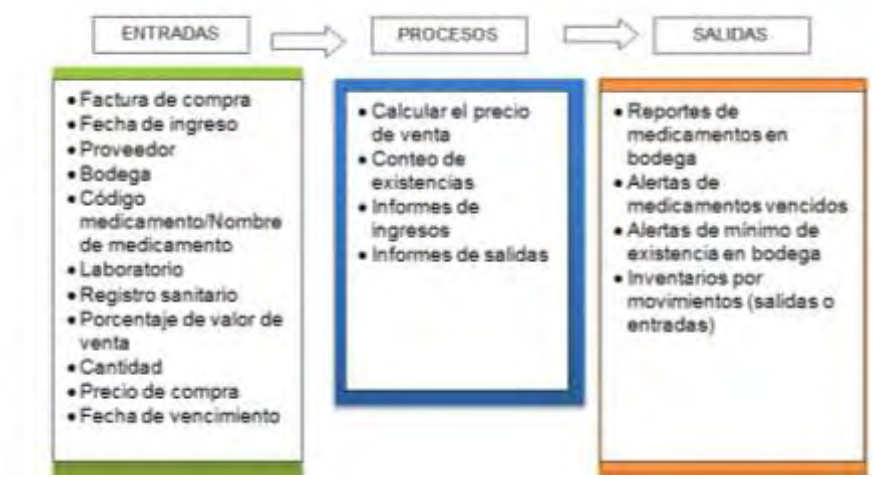



Figura 23. Cuadro funciones de módulo kardex. [1]

## 3.2 ARCHIVO CORRIENTE

Son documentos que soportan la labor y evidencias del proceso de auditoría, comprende la evaluación que hizo el auditor a la entidad, tales documentos son informes de pruebas, análisis, hallazgos, cuestionarios, programas de auditoría.

Con el fin de lograr un exitoso desarrollo del proceso de auditoría se realizó una recopilación de información y documentos necesarios para el conocimiento de la entidad y los procesos que allí se desarrollan.

### 3.2.1 Memorando de planeación de auditoría

**Objetivo general.** Evaluar los módulos correspondientes al software de gestión de información INFO-SALUD con el fin de establecer la confiabilidad e integridad de

la información, permitiendo realizar las respectivas recomendaciones que permitirán a la Institución adelantar actividades de mejoramiento, logrando así mejorar la prestación de servicios de salud a los usuarios.

**Alcance.** El desarrollo de esta auditoría contempla los módulos que conforman el software INFO-SALUD, mediante el cual se gestiona la información manejada en la IPS Indígena Guaitara. Para las debidas pruebas y evaluación de la misma se utilizó la metodología COBIT y técnicas de auditoría con el propósito de evaluar el correcto funcionamiento de este software.

Los módulos que se evaluaron en esta auditoría, fueron:

- Historianet
- Citas médicas
- Facturación (kardex)

A los módulos anteriormente mencionados, se evaluó la funcionalidad, procesamiento de entradas, salidas generadas por el sistema, calidad de los datos de entrada, la configuración del sistema, la administración del sistema y planes de contingencias.

En cuanto a la operatividad del sistema se evaluó los permisos y características de los usuarios que manejan la información, la administración y monitoreo del sistema.

**Metodología**

Para la recopilación de la información se utilizaron diferentes métodos:

**Visitas a:**

- Instalaciones físicas de la IPSI Guaitara
- Centro de informática

**Entrevistas a:**

Personal administrativo IPSI Guaitara

- Gerente general
- Director administrativo

- Medico auditor
- Funcionarios encargados de manejo de los módulos de INFO-SALUD (médicos, enfermeras, atención al usuario, odontólogos, encargados de farmacia y auxiliar de odontología)

Centro de informática:

- Personal administrador del centro de Informática Ingeniero Darío Burbano.

**Encuestas:**

- Encuesta general a funcionarios de la IPSI Guaitara encargados de operar los diferentes módulos de INFO-SALUD[98]

**Formularios:**

- Cuadros de definición aplicados a la auditoría
- Cuestionarios cuantitativos
- Cuestionarios cualitativos
- Evaluación módulos de software
- Valoración de riesgos
- Matriz de probabilidad e impacto
- Tabla de hallazgos

**3.2.2 Programa de auditoría.** Para la realización del proceso de auditoría a los módulos de facturación, consultas e historia clínica del software de administración y gestión de información INFO-SALUD se utilizó la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), y se evaluaron algunos objetivos de control que se encuentran dentro de los dominios de esta metodología así:

**Dominio: planeación y organización (PO).**

**PO1 Definir un plan estratégico TI.**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos

[98] Ver ANEXO F. Entrevistas_Preguntas_Cerradas

netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**PO2 Definir la arquitectura de la información.**

- **PO2.1 Modelo de arquitectura de información empresarial:** este objetivo de control no fue tomado en cuenta en la ejecución de esta auditoría dado que busca definir estrategias corporativas para el mejor funcionamiento de la entidad y no se enfoca al aplicativo informático analizado.

- **PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos:** se evaluó la existencia de un diccionario de datos, en el que se debe establecer definiciones precisas y rigurosas con el fin de:

  - ✓ Reducir redundancia de los datos
  - ✓ Identificar entradas, salidas y procedimientos
  - ✓ Prevenir datos incompatibles que maneja el aplicativo informático.

  La revisión se hizo al aplicativo en general mediante técnicas de:

  - ✓ Observación de entrada y salida de datos en el aplicativo informático.
  - ✓ Búsqueda de datos inconsistentes y duplicados.
  - ✓ Entrevistas realizadas al personal operario del aplicativo INFO-SALUD

- **PO2.3 Esquema de clasificación de datos:** se identificó si la entidad mantiene un esquema de datos en el que se especifique:

  - ✓ El nivel de confidencialidad de la información de la IPS
  - ✓ Propiedad de datos
  - ✓ Niveles de seguridad
  - ✓ Controles de protección
  - ✓ Procesos donde se emplean los datos

  En este análisis se utilizaron técnicas, como:

  - ✓ Access PassView, Software freeware para lograr el acceso a la base de datos y cuentas de usuario de INFO-SALUD.

- ✓ Entrevistas a los operarios del aplicativo informático con el fin de evaluar niveles de seguridad en las cuentas de INFO-SALUD.

- ✓ Entrevistas al Ingeniero encargado con el fin de analizar los planes de seguridad referentes al uso del aplicativo informático INFO-SALUD.

Esto con el propósito de observar la aplicación de controles de acceso y protección de la información.

- **PO2.4 Administración de integridad:** se evaluó si la entidad implementa procedimientos para a garantizar la integridad y consistencia de los datos almacenados, con el fin de:

  - ✓ Analizar los beneficios de implementar políticas de control de información con el fin de evitar la modificación de la información manejada en el aplicativo informático INFO-SALUD.

  La revisión se hizo al aplicativo INFO-SALUD y a los informes que de él se extraen, analizando:

  - ✓ Coherencia de informes electrónicos de INFO-SALUD y los documentos físicos que existen en la institución.

  - ✓ Entrevistas realizadas a los operarios de los módulos pertenecientes a INFO-SALUD con el fin de corroborar si la información es consistente según su criterio.

El análisis de los objetivos de control pertenecientes al proceso PO2 se evidencian en la aplicación, mediante:

- Definición de fuentes de conocimiento PO2
- Cuestionario cuantitativo PO2
- Cuadro de hallazgos PO2(1)
- Cuadro de hallazgos PO2(2)
- Cuadro de hallazgos PO2(3)
- Cuadro de valoración de riesgos
- Matriz de probabilidad e impacto

**PO3 Determinar la dirección tecnológica**

Este objetivo de control no fue tomado en cuenta en la ejecución de esta auditoría ya que busca generar planes estratégicos para el mejor desempeño de la institución y no se enfoca al aplicativo informático analizado.

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

- **PO4.1 Marco de trabajo de procesos de TI:** este objetivo no fue tomado en cuenta durante el desarrollo de esta auditoría dado que hace referencia a planes estratégicos de tecnologías de información los cuales son estrategias gerenciales que no se dirigen específicamente al aplicativo INFO-SALUD

- **PO4.2 Comité estratégico de TI:** este objetivo de control no fue tenido en cuenta puesto que se enfoca en planes estratégico para inversiones TI de la institución y no se enfoca al aplicativo informático analizado

- **PO4.3 Comité directivo de TI**: este objetivo de control está encaminado a definir las actividades del comité directivo de TI y no tiene relación con la temática analizada en el software INFO-SALUD.

- **PO4.4 Ubicación organizacional de la función TI:** este objetivo de control no es de importancia para el desarrollo de esta auditoría ya que se encamina a modelo de negocios los cuales no están dentro del desarrollo temático de la auditoría al aplicativo informático INFO-SALUD.

- **PO4.5 Estructura organizacional:** este objetivo no es tomado en cuenta dentro de esta auditoría puesto que es un proceso netamente gerencial de TI y no se enfoca al aplicativo informático analizado.

- **PO4.6 Establecimiento de roles y responsabilidades:** este objetivo de control corresponde a responsabilidades gerenciales, motivo por el cual no es tomado en cuenta dado que no tiene relación con el aplicativo informático INFO-SALUD.

- **PO4.9 Propiedad de datos y de sistemas:** se evaluó si la entidad tiene procedimientos y herramientas para identificar responsabilidades sobre los datos teniendo en cuenta los siguientes aspectos:

    - ✓ Personal responsable de la información.
    - ✓ Clasificación de la información privada o confidencial como las historias clínicas.

- ✓ Protección de la información confidencial.

Estos aspectos se analizaron mediante técnicas de auditoría como:

- ✓ Ingreso al aplicativo INFO-SALUD
- ✓ Observación de roles de los empleados
- ✓ Manuales de funciones
- ✓ Planes de seguridad donde se especifican limitación de la información.

- **PO4.10 Supervisión:** se inspeccionó si se Implementa prácticas adecuadas de supervisión de roles y las responsabilidades de los operarios de INFO-SALUD con el propósito de:

  Mantener un buen nivel en las actividades realizadas por los empleados encargados del manejo de los módulos del aplicativo informático INFO-SALUD.

  Mantener un continuo plan de inspección a los empleados encargados de actividades donde se maneje información sensible En el aplicativo informático.

  Este objetivo de control se analizó mediante:

  - ✓ Entrevistas con el Ingeniero encargado
  - ✓ Entrevistas a los operarios de INFO-SALUD.
  - ✓ Entrevista al personal administrativo encargado de implementar planes de seguridad.

- **PO4.11 Segregación de funciones:** se evaluó si en el área de sistemas se implementa una división de roles y responsabilidades, con el fin de:

  - ✓ Tener bien definidas las actividades que cada operario debe hacer en su módulo correspondiente.

  - ✓ Evitar por medio de protocolos de seguridad y confidencialidad, que operarios solo tenga ingreso al módulo y a la información que sea de si incumbencia.

  Esto se analizó mediante las siguientes actividades:

- ✓ Restricción de Información
- ✓ Controles de acceso
- ✓ Roles y contraseñas

- **PO4.12 Personal de TI:** se evaluó si existen procesos de evaluación para materiales de apoyo entregado a los operarios del aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Garantizar que las funciones realizadas por los operarios de del aplicativo informático cuenten con recursos que soporten adecuadamente sus funciones.

  Este objetivo de control se analizó mediante:

  - ✓ Análisis del manual de funciones del personal operario del software.
  - ✓ Análisis de los roles y responsabilidades del personal encargado del aplicativo informático.
  - ✓ Comparación de funciones documentadas con las funciones realizadas por los trabajadores.

- **PO4.13 Personal clave de TI:** se identificó el personal clave que desempeña funciones de trabajo críticas en la operación del aplicativo INFO-SALUD, con el fin de:

  - ✓ Evidenciar la dependencia en individuos que poseen altos conocimientos en el funcionamiento del aplicativo informático y sin los cuales la institución presentaría retrasos en algunos procesos manejados por INFO-SALUD.

  Lo anterior se analizó teniendo en cuenta los siguientes aspectos:

  - ✓ Aplicación de entrevistas al personal operario del software
  - ✓ Identificación del personal con mayor conocimiento en el funcionamiento del aplicativo informático.
  - ✓ Verificación de existencia de manuales de usuario del aplicativo.
  - ✓ Identificación de personal capacitado y no capacitado
  - ✓ Verificación de existencia de herramientas de ayuda suministrados a los operarios.

- **PO4.14 Políticas y procedimientos para personal contratado:** este objetivo de control corresponde a responsabilidades y políticas organizacionales, motivo por el cual no es tomado en cuenta dado que no tiene relación con el aplicativo informático INFO-SALUD.

- **PO4.15 Relaciones:** este objetivo de control no es tomado en cuenta ya que es responsabilidad de los directivos de la institución, los contratistas y la gerencia externa motivo por el cual no cumple con el objetivo al cual está encaminada esta auditoría el cual es el análisis del software INFO-SALUD.

El análisis de los objetivos de control pertenecientes al proceso PO4 se evidencia en la aplicación mediante:

- Definición de fuentes de conocimiento PO4
- Cuestionario cuantitativo PO4
- Cuadro de hallazgos PO4 (1)
- Cuadro de valoración de riesgos
- Matriz de probabilidad e impacto

**PO5 Administrar la inversión TI**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos de inversión en tecnología los cuales son procedimientos administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**PO6 Comunicar las aspiraciones y la dirección de la gerencia**

Este dominio no es analizado ya que corresponde a políticas y actividades de las cuales se encarga la gerencia y no el aplicativo informático INFO-SALUD el cual es el objeto de análisis de esta auditoría.

**PO7 Administrar los recursos humanos de TI**

- **PO7.1 Reclutamiento y retención del personal:** confirmar la existencia de procesos de reclutamiento de personal, con el fin de:

  - ✓ Evidenciar si los operarios tienen las habilidades necesarias para manejar apropiadamente los módulos del software INFO-SALUD.

Este objetivo de control se analizó considerando los siguientes aspectos:

- ✓ Observación de desempeño del personal encargado de los módulos que conforman el aplicativo informático INFO-SALUD.

- ✓ Análisis de políticas de entrenamiento al personal operario de los módulos de INFO-SALUD.

- ✓ Comprobación de existencia de material de ayuda para entrenamiento del personal operario del aplicativo informático.

- **PO7.2 Competencias del personal:** se analizó el desempeño del personal encargado del manejo de los módulos del aplicativo informático INFO-SALUD, con la finalidad de:

  - ✓ Lograr una mejor calidad en las actividades realizadas por los trabajadores encargados de los procesos manejados en INFO-SALUD.

  Este aspecto se analizó teniendo en cuenta los siguientes aspectos:

  - ✓ Existencia de políticas de evaluación de desempeño del personal.

  - ✓ Análisis de requisitos de educación, entrenamiento y/o experiencia.

  - ✓ Análisis de políticas de entrenamiento al personal encargado de operar los módulos del aplicativo informático.

- **PO7.3 Asignación de roles:** este objetivo de control hace alusión a procedimientos administrativos que no están orientadas al funcionamiento del aplicativo informático INFO-SALUD, motivo por el cual no fue tomado en cuenta en el desarrollo de esta auditoría.

- **PO7.4 Entrenamiento del personal de TI:** se analizaron los procedimientos de entrenamiento brindados al personal que se encargará de operar los módulos de INFO-SALUD, con la finalidad de:

  - ✓ Lograr un mejor nivel de conocimiento de los procedimientos que se gestionan en el aplicativo informático INFO-SALUD.

  - ✓ Evitar perdida de información debido a un mal manejo en los procesos del aplicativo Informático.

  Esto se evaluó teniendo en cuenta los siguientes aspectos:

- ✓ Planes de entrenamiento continúo al personal encargado del aplicativo informático.
- ✓ Implementación de políticas orientadas a conservar el conocimiento de los empleados encargados del funcionamiento del software.

- ✓ Aplicación de procedimientos sobre la seguridad y confidencialidad de la información manejada en el aplicativo informático.

- ✓ Análisis si el personal encargado de la operación de los módulos del aplicativo poseen conocimientos básicos sobre informática.

- **PO7.5 Dependencia sobre los individuos:** se evaluaron procedimientos para evitar la dependencia hacia el personal que posee altos conocimientos acerca del funcionamiento del aplicativo informático INFO-SALUD.

  Este objetivo de control se analizó con el fin de:

  - ✓ Evaluar el nivel de dependencia hacia individuos con gran conocimiento en el software por medio de políticas para compartir el conocimiento, capacitaciones y documentación sobre el aplicativo informático.

  Esto se analizó considerando los siguientes aspectos:

  - ✓ Existencia de manuales de usuario para los operarios de los módulos del software.

  - ✓ Captura del conocimiento de los empleados (documentación, bitácora de errores y posibles soluciones)

  - ✓ Fechas en las cuales se realizaron capacitaciones al personal encargado del manejo del aplicativo informático.

  - ✓ Planes de desvinculación de personal.

- **PO7.6 Procedimientos de investigación del personal:** Este objetivo de control no fue tomado en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

- **PO7.8 Cambios y terminación de trabajo:** En este objetivo de control se analizaron las políticas de seguridad que se toman en la institución cuando existe terminación del contrato de algún operario del aplicativo INFO-SALUD.

Lo anterior se analizó mediante:

- ✓ Análisis de la existencia y práctica de políticas de administración de privilegios de acceso al Software INFO-SALUD.

Estas políticas buscan que al personal que termine su contrato con la IPS se le restrinja el acceso al software a fin de minimizar los riesgos de divulgación, pérdida y daño de información.

El análisis de los objetivos de control pertenecientes al proceso PO7 se evidencia en la aplicación mediante:

- ✓ Definición de fuentes de conocimiento PO7
- ✓ Cuestionario cuantitativo PO7
- ✓ Cuadro de hallazgos PO7 (1)
- ✓ Cuadro de hallazgos PO7 (2)
- ✓ Cuadro de hallazgos PO7 (3)
- ✓ Cuadro de hallazgos PO7 (4)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**PO8 Administrar la calidad**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

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

- **PO9.1 Marco de trabajo de administración de riesgos:** la presente auditoría no tiene como objetivo analizar políticas de administración de la institución, por este motivo este objetivo de control no se considera de importancia en el desarrollo de este trabajo.

- **PO9.2 Establecimiento del contexto de riesgo**: no se tomó como objeto de análisis este objetivo de control ya que analiza procesos administrativos de riegos, por lo cual no tiene relación con el funcionamiento del software INFO-SALUD.

- **PO9.3 Identificación de eventos:** se evaluó la existencia procedimientos que permitan identificar vulnerabilidades en el aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Implementar procedimientos de mitigación de riesgos que puedan afectar el buen funcionamiento y la integridad de la información administrada en el aplicativo informático INFO-SALUD.

  Se evaluaron los siguientes aspectos:

  - ✓ Existencia de una bitácora de errores en donde se registren los riesgos relevantes y su incidencia.

  - ✓ Existencia de procesos donde se especifique tiempos de respuesta a riesgos que se puedan presentar en el aplicativo informático..

- **PO9.4 Evaluación de riesgos de TI:** se revisó si se evalúa la periodicidad con la que se analizan impactos negativos y su probabilidad de ocurrencia en el aplicativo informático.

  La finalidad del análisis de este objetivo de control es evidenciar las fallas en los procedimientos de predicción y análisis de riesgos que puedan generar fallas en los servicios gestionados por el aplicativo informático.

  Lo anterior teniendo en cuenta:

  - ✓ Existencia de documentación donde se especifiquen los riesgos, motivo del riesgo que puedan afectar el buen desempeño de los procesos gestionados por el aplicativo informático INFO-SALUD.

- **PO9.5 Respuesta a los riesgos:** se evaluó la existencia de un proceso de respuesta a riesgos que puedan presentarse en el aplicativo informático INFO-SALUD, con el fin de:

  - ✓ Identificar las posibles amenazas que afectarían el buen desempeño del aplicativo informático INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta los siguientes aspectos:

  - ✓ Implementación de estrategias para evitar, reducir o identificar riesgos

- ✓ Determinar las responsabilidades que tienen los operarios del aplicativo en la manifestación de riesgos.

- ✓ Actividades para establecer niveles de tolerancia a riesgos.

- **PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos:** se analizó si existen actividades encaminadas a la implementación y mantenimiento de planes de respuesta a riesgos.

  - ✓ Enfatizar en la importancia de implementar, diseñar y monitorear un plan de acción de riesgo que puedan afectar el correcto funcionamiento del aplicativo INFO-SALUD y la integridad de la información que en este se gestiona.

  Este análisis se logró mediante la realización de las siguientes actividades:

  - ✓ Evaluar la existencia de actividades de control para mitigar los riesgos identificados.

  - ✓ Identificar al personal responsable de ejecutar el plan acción de riesgos.

  - ✓ Análisis si el plan de riesgos implementado en la institución es adecuado teniendo en cuenta las necesidades de las dependencias en las que se maneja el aplicativo informático.

- **PO9.10 Administrar proyectos:** la presente auditoría no tiene como objetivo analizar políticas de administración de la institución, por este motivo este objetivo de control no se considera de importancia en el desarrollo de este trabajo.

El análisis de los objetivos de control pertenecientes al proceso PO9 se evidencia en la aplicación mediante:

- Definición de fuentes de conocimiento PO9
- Cuestionario cuantitativo PO9
- Cuadro de hallazgos PO9 (1)
- Cuadro de hallazgos PO9 (2)
- Cuadro de valoración de riesgos
- Matriz de probabilidad e impacto

**Dominio: adquirir e implementar (AI)**

**AI1 Identificar soluciones automatizadas**

- **AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.** Se analizó si en la institución se cumplió un proceso en el cual se evaluó los requerimientos técnicos y funcionales antes de la adquisición del aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Garantizar que mediante un proceso formal de requerimientos las necesidades del negocio estén completas y detalladas, con el fin de lograr identificar la mejor opción a la hora de adquirir una herramienta informática.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Evaluar la existencia de documentación en donde se especifiquen requerimientos funcionales y técnicos que cubran las necesidades de la institución

  - ✓ Entrevistas con el personal administrativo, medico auditor e ingeniero encargado con el fin de analizar si se realizó un proceso de adquisición de software y si este cumple con las necesidades de la institución.

- **AI1.2 Reporte de análisis de riesgos:** este objetivo de control no fue tomado en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos organizacionales de los cuales está encargada la gerencia y no se enfocan al funcionamiento del software INFO-SALUD.

- **AI1.3 Estudio de factibilidad y formulación de cursos de acción alternativos**: se evaluó si existió un estudio de factibilidad antes de la adquisición del aplicativo informático INFO-SALUD, con el fin de:

  - ✓ Evaluar que durante el análisis de compra se estableció un proceso formal donde se detallen los requerimientos que tiene la institución y que debían ser soportados por el aplicativo informático.

  Lo anterior se evaluó teniendo en cuenta las siguientes actividades:

  - ✓ Evaluar la existencia de un proceso de aceptación del software o un plan de implementación de nuevos requisitos.

- ✓ Aplicación de entrevistas a los operarios de los módulos del aplicativo informático con el fin de analizar si el software cumple con los requerimientos necesarios para la prestación de un buen servicio a los usuarios.

- ✓ Aplicación de entrevistas al ingeniero encargado y medico auditor con el fin de obtener opiniones fundamentadas acerca del cumplimiento de requerimientos y funcionamiento del aplicativo informático.

- **AI1.4 Fiabilidad y aprobación:** se analizó la existencia de un proceso de aprobación para la adquisición del software INFO-SALUD, esto con el fin de:

  - ✓ Soportar de manera legal la aprobación el cumplimiento de los requerimientos solicitados por la institución prestadora de servicio a la hora de aprobar la adquisición de aplicativo informático.

  Este objetivo de control se analizó por medio de las siguientes actividades:

  - ✓ Aplicación de entrevistas a personal administrativo el cual es el encargado de la aprobación de adquisiciones.

  - ✓ Aplicación de entrevistas al ingeniero encargado y representantes de las dependencias que se encargan de la operación del aplicativo informático INFO-SALUD

El análisis de los objetivos de control pertenecientes al proceso AI1 se evidencia en la aplicación mediante:

- Definición de fuentes de conocimiento AI1
- Cuestionario cuantitativo AI1
- Cuadro de hallazgos AI1 (1)
- Cuadro de hallazgos AI1 (2)
- Cuadro de valoración de riesgos
- Matriz de probabilidad e impacto

**AI2 Adquirir y mantener software aplicativo**

- **AI2.1 Diseño de alto nivel:** este objetivo de control no fue tomado en cuenta para el análisis de esta auditoría ya que hacen referencia a

procesos organizacionales de los cuales está encargada la gerencia y no se enfocan al funcionamiento del software INFO-SALUD.

- **AI2.2 Diseño detallado:** este objetivo de control no fue tomado en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos organizacionales de los cuales está encargada la gerencia y no se enfocan al funcionamiento del software INFO-SALUD.

- **AI2.3 Control y posibilidad de auditar las aplicaciones de la organización:** este objetivo de control es llevado a cabo por la dependencia de auditoria Interna, motivo por el cual no es tomado en cuenta en esta auditoría ya que está enfocada al aplicativo informático INFO-SALUD.

- **AI2.4 Seguridad y disponibilidad de aplicaciones:** se evaluaron protocolos de seguridad implementados para la protección y disponibilidad de la información gestionada por el aplicativo informático INFO-SALUD, esto con la finalidad de:

  - ✓ Garantizar integridad, disponibilidad y confidencialidad en la información y procesos de INFO-SALUD.

  Las actividades que se analizaron incluyen:

  - ✓ Análisis de derechos de acceso y administración de privilegios en el aplicativo informático.

  - ✓ Verificación de existencia de procesos de protección de información sensible gestionada por INFO-SALUD.

  - ✓ Verificación de autenticación de acceso a los módulos e integridad de las transacciones.

- **AI2.5 Configuración e implantación de software aplicativo adquirido:** se analizaron las políticas de implementación de software INFO-SALUD con el fin de conseguir el adecuado funcionamiento del aplicativo informático.

  Las actividades que se tomaron en cuenta para el análisis de este objetivo, son:

  - ✓ Se analizó si el software cumple los requisitos mínimos exigidos por los procesos realizados en cada dependencia.

  - ✓ Revisión de documentación técnica y manuales de usuario.

- ✓ Revisión planes de prueba realizados para la adquisición del aplicativo.

- **AI2.6 Actualizaciones importantes en sistemas existentes:** se comprobó si existe un proceso formal para solicitar cambios importantes en la funcionalidad del aplicativo INFO-SALUD, con el fin de:

  - ✓ Priorizar módulos o funcionalidades que deben ser actualizados mediante un proceso formal de solicitud al proveedor del aplicativo informático.

  Los aspectos a considerar en el análisis de este objetivo incluyen:

  - ✓ Existencia de un proceso para solicitar cambio en el aplicativo INFO-SALUD.

  - ✓ Verificación si el proceso de cambio incluye aspectos como análisis de necesidad del cambio, justificación costo/beneficio y administración de requerimientos.

  - ✓ Análisis de tiempo de respuestas a cambios en el aplicativo informático.

- **AI2.7 Desarrollo de software aplicativo:** este objetivo de control no fue tomado en cuenta para el análisis de esta auditoría ya que no se enfoca al funcionamiento del software INFO-SALUD

- **AI2.8 Aseguramiento de calidad de software:** se evaluó si se desarrolló un plan de medición de la calidad del aplicativo informático INFO-SALUD antes de su adquisición, con el fin de:

  - ✓ Garantizar calidad en la prestación del servicio a los usuarios, ya que la información gestionada por el aplicativo tendrá un buen nivel de seguridad, integridad y confidencialidad en la información.

  Para el análisis de este objetivo de control se realizaron las siguientes actividades:

  - ✓ Análisis de existencia de políticas de cumplimiento de requerimientos antes de la adquisición del aplicativo INFO-SALUD.

  - ✓ Evaluar el cumplimiento de estándares de calidad como funcionalidad, confiabilidad, eficiencia, usabilidad, mantenibilidad y portabilidad del software.

- ✓ Aplicación de entrevistas a los operarios con el fin de analizar los niveles de satisfacción de estos con el aplicativo informático INFO-SALUD.

- **AI2.9 Administración de los requerimientos de aplicaciones:** se evaluó la existencia de procesos de seguimiento de requerimientos antes y después de la adquisición del aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Garantizar el cumplimiento de necesidades de cargas de trabajo, concurrencia, seguridad, e integridad de la información por parte del aplicativo informático.

  - ✓ Evaluar el correcto funcionamiento del aplicativo durante un periodo de prueba en el ambiente real de la institución.

  Los aspectos a considerar en el análisis de este objetivo incluyeron:

  - ✓ Entrevistas al ingeniero encargado, representantes de dependencias y personal administrativo con el fin de recolectar información con respecto al proceso de adquisición del software INFO-SALUD.

  - ✓ Comprobar la existencia de un proceso formal de gestión requerimientos para identificar para la adquisición, actualizaciones e implementación de nuevos necesidades sobre el aplicativo informático.

- **AI2.10 Mantenimiento de software aplicativo:** se analizó el proceso que se lleva a cabo para realizar el mantenimiento del aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Evitar problemas que puedan afectar en un futuro la prestación del servicio, la integridad y la seguridad de la información que se gestiona en el aplicativo informático INFO-SALUD.

  Para el análisis de este objetivo se tuvieron en cuenta las siguientes actividades:

  - ✓ Evaluar la existencia de protocolos para la mejora y optimización del aplicativo informático.

  - ✓ Se analizó si el plan de mantenimiento cubre aspectos como razón de solicitud del mantenimiento, responsable asignado para realizar el mantenimiento, actividades a realizar durante el mantenimiento y

periodicidad con que es necesario realizar mantenimiento al aplicativo

El análisis de los objetivos de control pertenecientes al proceso AI2 se evidencia en la aplicación mediante:

- ✓ Definición de fuentes de conocimiento AI2
- ✓ Cuestionario cuantitativo AI2
- ✓ Cuadro de hallazgos AI2 (1)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**AI3 Adquirir y mantener infraestructura tecnológica**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**AI4 Facilitar la operación y el uso**

- **AI4.1 Plan para soluciones de operación:** este objetivo de control no fue tomado en cuenta en la ejecución de esta auditoría dado que busca definir estrategias corporativas para el mejor funcionamiento de la entidad y no se enfoca al aplicativo informático analizado.

- **AI4.2 Transferencia de conocimiento a la gerencia del negocio:** no es competencia de esta auditoría analizar procedimientos administrativos motivo por el cual no se tomó en cuenta para el desarrollo de este trabajo de grado.

- **AI4.3 Transferencia de conocimiento a usuarios finales:** se evaluó si la institución tiene implementado un plan de entrenamiento para los operarios de los módulos del aplicativo informático INFO-SALUD, con la finalidad de:

  - ✓ Lograr que el personal encargado del manejo del aplicativo esté mejor preparado, adiestrado, lo cual hará que el desarrollo en sus actividades sea eficaz y eficiente.

  Para el estudio de este objetivo se tuvo en cuenta las siguientes actividades:

- ✓ Análisis de los procesos de transferencia de conocimiento a los operarios del aplicativo informático.

- ✓ Se evaluó si existen materiales de entrenamiento como manuales de usuario, manuales de procedimientos, y apoyo a los operarios de los módulos del software INFO-SALUD.

- ✓ Aplicación de entrevistas con el fin de conocer el nivel de satisfacción de los operarios con las políticas de entrenamiento impartidas.

- **AI4.4 Transferencia de conocimiento al personal de operaciones y soporte:** se evalúo la existencia de planes de entrenamiento enfocado al personal técnico, encargado del aplicativo informático INFO-SALUD, esto con el fin de que el personal del área de informática posea los conocimientos técnicos acerca de la aplicación informática necesarios para resolver con rapidez cualquier falla, minimizando así los inconvenientes generados en la institución.

  Las actividades realizadas para el análisis de este objetivo de control incluyeron:

  - ✓ Análisis de plan de entrenamiento suministrado por el ingeniero desarrollador al Ingeniero de sistemas de la IPSI ya que él es parte del personal encargado de dar soporte al aplicativo informático al momento de presentarse fallas.

  - ✓ Evaluar la existencia de documentación como manuales técnicos, diagramas de flujo de la información, o pseudocódigo del aplicativo informático.

  El análisis de los objetivos de control pertenecientes al proceso AI4 se evidencia en la aplicación mediante

  - Definición de fuentes de conocimiento AI4
  - Cuestionario cuantitativo AI4
  - Cuadro de hallazgos AI4 (1)
  - Cuadro de valoración de riesgos
  - Matriz de probabilidad e impacto

**AI5 Adquirir recursos TI**

Este dominio no es tomado en cuenta para en el desarrollo de esta auditoría ya que hace referencia a procesos administrativos para la adquisición de tecnología y no se enfoca al funcionamiento del aplicativo informático INFO-SALUD.

**AI6 Administrar cambios**

- **AI6.1 Estándares y procedimientos para cambios:** se evaluó existencia de procedimientos para para la administración de cambios en el software, con el fin de:

  - ✓ Organizar proceso formal para solicitud de cambios en el aplicativo informático INFO-SALUD, teniendo en cuenta prioridades en los procesos gestionados por la aplicación.

  Para el análisis de este objetivo de control se tuvo en cuenta las siguientes actividades:

  - ✓ Se analizó si los procesos de gestión de cambios son concertados entre la institución y el ingeniero desarrollador teniendo en cuenta la prioridad de cada actualización.

  - ✓ Se aplicaron entrevistas al personal operario de aplicativo informático con el fin de conocer el proceso que se lleva a cabo para la implantación de actualizaciones y la entrega de la respectiva documentación acerca del cambio.

- **AI6.2 Evaluación de impacto, priorización y autorización:** este objetivo de control no ha sido tomado en cuenta para el desarrollo de esta auditoría, ya que está enfocado hacia los procesos que deben ser aprobados y ejecutados por la gerencia por lo tanto no hace referencia al funcionamiento del aplicativo informático INFO-SALUD.

- **AI6.3 Cambios de emergencia:** se evaluó si se tiene estableció un proceso para definir y autorizar los cambios de emergencia.

  Este objetivo de control se analizó, mediante las siguientes actividades:

  - ✓ Se verificó la existencia de un proceso formal de priorización de cambios en el aplicativo informático INFO-SALUD.

  - ✓ Se analizó el proceso realizado en la institución para la solicitud de cambios al proveedor del aplicativo informático INFO-SALUD.

- **AI6.4 Seguimiento y reporte de estatus de cambio:** este objetivo de control no fue tomado en cuenta en el desarrollo de esta auditoría ya que hace parte de los procesos que debe seguir el desarrollador del aplicativo ya que a la institución le interesa que se tome en cuenta el cambio y que posteriormente se implante mas no el estado del cambio durante el desarrollo.

- **AI6.5 Cierre y documentación del cambio:** se analizó si en la entidad se establece un proceso de revisión post-implantación del aplicativo informático INFO-SALUD, esto con la finalidad de:

  - ✓ Evaluar la implantación completa de los cambios solicitados al proveedor del aplicativo, así como los resultados del plan de pruebas realizado antes de aceptar el cambio.

  Para el análisis de este objetivo de control se tuvo en cuenta las siguientes actividades:

  - ✓ Verificación de existencia en un protocolo post-implantación que busque asegurar el correcto funcionamiento del aplicativo informático.

  - ✓ Verificación de la existencia de un protocolo para la aplicación de pruebas al cambio hecho en el aplicativo informático.

El análisis de los objetivos de control pertenecientes al proceso AI6 se evidencia en la aplicación mediante

- ✓ Definición de fuentes de conocimiento AI6
- ✓ Cuestionario cuantitativo AI6
- ✓ Cuadro de hallazgos AI6 (1)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**AI7 Instalar y acreditar soluciones y cambios**

- **AI7.1 Entrenamiento:** se evaluó, si existen políticas de entrenamiento al personal encargado de la operación de los módulos del aplicativo INFO-SALUD al momento de su implantación y/o actualización, con el fin de:

  - ✓ Contar con un personal calificado en la operación de los respectivos procesos trabajados en el aplicativo INFO-SALUD.

- ✓ Mejorar el rendimiento productivo, mediante la mejora de las habilidades, actitudes y conocimientos en el manejo del aplicativo informático.

Este objetivo de control se analizó mediante las siguientes actividades:

- ✓ Se analizó la existencia de procesos de capacitación y entrenamiento al personal encargado de la operación de los módulos de INFO-SALUD.

- ✓ Se comprobó la existencia de documentación técnica y manuales de usuario de los cambios hechos al aplicativo informático.

- ✓ Se evaluó mediante entrevistas con el ingeniero encargado la existencia de documentación técnica de las actualizaciones así como manuales de usuario.

- **AI7.2 Plan de prueba:** se evaluó si se estableció un plan de pruebas basado en los procesos soportados por el software de INFO-SALUD y requerimientos de entrada y salida, con el fin de:

  - ✓ Garantizar la implantación completa de los requisitos que el aplicativo informático debe cumplir.

  - ✓ Garantizar la continuidad del servicio en el aplicativo INFO-SALUD.

  - ✓ Evaluar la calidad y el funcionamiento del software INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Se analizó, si se realizó un proceso para establecer un periodo de prueba después de la implantación del cambio hecho al software.

  - ✓ Se analizó, si en el plan de pruebas se establecen actividades como localizar errores, analizar soluciones, solicitar la reparación del error y re-testear el aplicativo informático.

  - ✓ Se analizó, si durante el plan de pruebas se tuvo en cuenta a los representantes de las dependencias donde se opera el aplicativo informático.

- ✓ Se evaluó la existencia de documentación de especificación de requerimientos de sistema. y especificación de requerimientos de software (Diagrama de casos de uso).

- **AI7.3 Plan de implantación:** se evaluó si existió un plan de implantación formal donde se definan las tareas o agenda de implantación del aplicativo informático INFO-SALUD, con el fin de:

  - ✓ Tener un proceso detallado donde se describan aquellos recursos necesarios para llevar a cabo una correcta implantación del sistema INFO-SALUD.

  - ✓ Tener la seguridad de que el aplicativo informático adquirido es totalmente operativo.

  Para el estudio de este objetivo se tuvo en cuenta las siguientes actividades:

  - ✓ Se verificó la existencia de un plan de implantación para el aplicativo informático INFO-SALUD el cual debe tener bien definido actividades como recursos necesarios de software y hardware mínimos necesarios para la instalación del aplicativo, pruebas para comprobar que el sistema esté totalmente operativo, proceso de entrenamiento del personal encargado de operar los módulos de INFO-SALUD, plan de soporte técnico donde el proveedor se compromete a asistir a los operarios del aplicativo informático en el uso correcto del sistema y a corregir las fallas que se presenten durante el periodo de prueba.

  - ✓ Se realizaron entrevistas al ingeniero encargado del centro de informática de la IPSI con el fin de evaluar si el proceso de implementación anteriormente descrito se realizó satisfactoriamente.

  - ✓ Se realizaron entrevistas al personal encargado del aplicativo informático con el fin de evaluar si se realizó un proceso de capacitación y asistencia por parte del proveedor del aplicativo informático INFO-SALUD.

- **AI7.4 Ambiente de prueba:** se revisó si se estableció un ambiente de pruebas para el aplicativo informático INFO-SALUD que se acerque al ambiente real de la institución, esto con el fin de:

  - ✓ Asegurar el correcto funcionamiento del aplicativo en un ambiente similar al que se manejará en la IPSI.

- ✓ Certificar niveles de seguridad, calidad en la información y cargas de trabajo que debe cumplir el aplicativo informático INFO-SALUD.

- ✓ Iniciar un proceso de solicitud de correcciones en caso que el aplicativo informático no cumpla con los requerimientos anteriormente acordados.

Para el estudio de este objetivo se tuvo en cuenta las siguientes actividades:

- ✓ Se verificó si existe un plan de pruebas en el que se establece que el ambiente en donde se ejecutan las pruebas al aplicativo informático es similar al ambiente de producción.

- ✓ Se analizó si se prepararon los datos de prueba que se requieren para la ejecución de las pruebas.

- ✓ Se analizaron las cargas de trabajo que soporta la base de datos utilizada por el aplicativo informático según especificaciones técnicas de Microsoft.

- ✓ Se evaluó la existencia de un plan de correcciones para remediar los errores significativos que se presentan durante el proceso de pruebas al aplicativo informático INFO-SALUD.

- **AI7.5: Conversión de sistemas:** este objetivo de control no ha sido tomado en cuenta para el desarrollo de esta auditoría, ya que está enfocado hacia los procesos que deben ser aprobados y ejecutados por la gerencia por lo tanto no hace referencia al funcionamiento del aplicativo informático INFO-SALUD.

- **AI7.6: Pruebas de cambios:** se analizó si existe un plan para evaluar si los cambios o actualizaciones en el aplicativo informático se ejecutan de manera satisfactoria, esto con el fin de:

  - ✓ Garantizar que los cambios implementados en el aplicativo informático INFO-SALUD trabajen de manera adecuada.

  - ✓ Evitar que los procesos gestionados por INFO-SALUD se tornen ineficientes debido al inadecuado funcionamiento del aplicativo informático.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

- ✓ Se evaluó si existen protocolos de aceptación de actualizaciones en el aplicativo INFO-SALUD.

- ✓ Se evaluó si existen planes de prueba para garantizar el correcto funcionamiento del aplicativo informático después de una actualización.

- **AI7.7 Prueba de aceptación final:** se analizó, si la entidad cuenta con planes de pruebas funcionales finales y si se aplicaron estas pruebas al aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Asegurar la implementación completa de los requerimientos solicitados por la institución prestadora de servicios de salud.

  - ✓ Asegurar el correcto funcionamiento del aplicativo informático INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Se analizó la existencia de planes de aceptación en donde se deben tener en cuenta aspectos como instalación, funcionalidad, validaciones, niveles de seguridad, información de salida y cargas de trabajo del aplicativo informático.

  - ✓ Se evaluó si el plan de pruebas funcionales analiza documentación técnica (diagramas de diseño, pseudocódigo, diagramas de entrada y salida de datos), manuales de instalación y de usuario para la instalación, mantenimiento y uso correcto de aplicativo INFO-SALUD.

  - ✓ Se aplicaron entrevistas al ingeniero encargado del centro de informática de la IPSI Guaitara con el fin de analizar el plan de pruebas aplicado al aplicativo informático.

  - ✓ Se aplicaron entrevistas a los operarios encargados de los módulos pertenecientes a INFO-SALUD con el fin de evaluar la existencia de manuales de usuario del aplicativo INFO-SALUD.

- **AI7.8 Promoción a producción:** se evaluó la existencia de procedimiento formal para el seguimiento y aprobación del plan de pruebas aplicado al software INFO-SALUD, esto con el fin de:

- ✓ Garantizar el nivel de satisfacción de operarios y parte Administrativa con los procedimientos soportados por el aplicativo informático INFO-SALUD.

- **AI7.9 Revisión posterior a la implantación:** se evaluó si existen procedimientos para realizar seguimiento al aplicativo INFO-SALUD después de su implementación en la institución, esto con el fin de:

  - ✓ Llevar un documento formal donde se evidencie el rendimiento de la aplicación con cargas de trabajo reales.

  Esto se analizó mediante las siguientes actividades:

  - ✓ Aplicación de entrevistas al Ingeniero encargado del centro de informática de la institución con el fin de evaluar la existencia de un plan post implantación para el aplicativo informático.

  - ✓ Aplicación de entrevistas a los operarios del software con el fin de evaluar la existencia de un plan post implantación para el aplicativo informático.

  - ✓ Evaluar la existencia de planes de aceptación de funcionalidad, y de manuales para el software INFO-SALUD por parte del personal administrativo, ingeniero encargado del centro de informática y representante de las dependencias en donde se utilizará el aplicativo informático.

El análisis de los objetivos de control pertenecientes al proceso AI7 se evidencia en la aplicación mediante

- ✓ Definición de fuentes de conocimiento AI7
- ✓ Cuestionario cuantitativo AI7
- ✓ Cuadro de hallazgos AI7 (1)
- ✓ Cuadro de hallazgos AI7 (2)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**Dominio: entregar y dar soporte (DS)**

**DS1 definir y administrar los niveles de servicio**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**DS2 Administrar los servicios de terceros**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría hacen parte de la gestión de la gerencia, en consecuencia no es parte de estudio de esta auditoría.

**DS3 Administrar el desempeño y la capacidad**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría estos planes son generados y aprobados por el personal administrativo de la IPSI y no hacen parte del análisis del aplicativo informático INFO-SALUD.

**DS4 Garantizar la continuidad del servicio**

- **DS4.1 Marco de trabajo de continuidad de TI:** este objetivo de control no ha sido tomado en cuenta para el desarrollo de esta auditoría, ya que está enfocado hacia los procesos que deben ser aprobados y ejecutados por la gerencia por lo tanto no hace referencia al funcionamiento del aplicativo informático INFO-SALUD.

- **DS4.2 Planes de continuidad de TI:** Se revisó la existencia de planes de continuidad fórmales a ejecutar en caso de fallas en el aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Garantizar la presentación continua del servicio de salud en la IPSI Guaitara a pesar de presentarse fallas en el aplicativo.

  - ✓ Lograr un buen nivel de respuestas por parte de los operarios del aplicativo a la hora de presentarse fallas en el software.

  - ✓ Lograr la pronta recuperación de la operación del aplicativo informático.

Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

- ✓ Se realizaron entrevistas aplicadas al ingeniero encargado del área de sistemas con el fin de evaluar la existencia de un plan de continuidad activo, vigente y actualizado

- ✓ Se analizó el contenido del plan de continuidad y los procedimientos alternativos que se deben ejecutar en caso de fallas en los servicios gestionados por INFO-SALUD.

- ✓ Se analizó la metodología de entrenamiento para ejecutar el plan de contingencia implementada con los funcionarios encargados del manejo de los módulos del aplicativo informático INFO-SALUD.

- ✓ Se aplicaron entrevistas al personal encargado de los módulos del aplicativo informático con el fin de evaluar la existencia de plan de contingencia en caso de fallas en el aplicativo INFO-SALUD.

- ✓ Se analizó si el plan de continuidad implementado posee distinción de niveles de prioridad en los procesos gestionados por cada uno de los módulos que conforman el aplicativo para la recuperación priorizada del servicio.

- **DS4.3 Recursos críticos de TI:** este objetivo de control no fue tomado en cuenta debido a que está dirigido a administración de recursos TI de toda la institución y no se enfoca exclusivamente al aplicativo informático INFO-SALUD.

- **DS4.4 Mantenimiento del plan de continuidad**: se analizaron los procedimientos para implementar de cambios en el plan de continuidad, esto con el fin de:

  - ✓ Mantener el plan de continuidad actualizado, teniendo en cuenta prioridades en los procedimientos llevados en el aplicativo informático INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Entrevistas con el ingeniero encargado del área de sistemas, con el fin de analizar las actividades que se realizan al plan de contingencia, teniendo en cuenta procesos cambiantes en la institución.

- **DS4.5 Pruebas del plan de continuidad:** se analizó si se implementó un protocolo de pruebas para el plan de continuidad, esto con el fin de:

  - ✓ Hacer evidentes las vulnerabilidades encontradas en este.

  - ✓ Implementar las correcciones pertinentes con el fin de cubrir la totalidad de las situaciones de riesgo en cuanto a prestación de servicios que se puedan presentar durante una falla en el aplicativo informático y así asegurar su efectividad en casos de desastre.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Entrevistas aplicadas al ingeniero encargado del área de sistemas, con el fin de evaluar la existencia de protocolos de pruebas aplicados al plan de contingencia enfocado a la aplicación informática INFO-SALUD.

- **DS4.6 Entrenamiento del plan de continuidad de TI:** se analizó la existencia de planes de entrenamiento aplicados al personal encargado de la operación de los módulos del aplicativo informático INFO-SALUD, esto se consideró con el fin de:

  - ✓ Lograr un buen nivel de respuesta a caídas del sistema por parte de los operarios con el fin de mitigar el impacto que tienen en la prestación del servicio de salud las fallas del aplicativo INFO-SALUD.

  Este objetivo de control se estudió teniendo en cuenta las siguientes actividades:

  - ✓ Se evaluó si los operadores de los módulos del aplicativo recibieron sesiones de entrenamiento enfocadas a procedimientos de contingencia aplicados durante la falla del aplicativo informático.

  - ✓ Se aplicaron entrevistas a los operarios con el fin de evaluar el conocimiento que poseen acerca de los protocolos de contingencia que deben seguir en caso de fallas en INFO-SALUD.

- **DS4.7 Distribución de un plan de continuidad**: este objetivo de control no ha sido tomado en cuenta para el desarrollo de esta auditoría, ya que está enfocado hacia los procesos que deben ser aprobados y ejecutados por la gerencia por lo tanto no hace referencia al funcionamiento del aplicativo informático INFO-SALUD.

- **DS4.8 Recuperación y reanudación de los servicios:** se evaluó la existencia de protocolos de recuperación de los servicios de los módulos del aplicativo informático al momento de presentarse fallas, esto con el fin de:

  - ✓ Mantener o recuperar los procesos llevados en el aplicativo INFO-SALUD, asegurando la disponibilidad de la información en el menor tiempo posible.

  Este objetivo de control se analizó teniendo en cuenta:

  - ✓ Se aplicó entrevistas al ingeniero encargado del área de sistemas con el fin de analizar los mecanismos de reanudación de servicios aplicados para una rápida respuesta al momento de presentarse una falla en INFO-SALUD.

  - ✓ Se analizaron tiempos de respuesta, actualización de información llevada en los mecanismos de respaldo y pruebas de funcionamiento con el fin de asegurase de que el aplicativo informático y la información que allí se maneja consistente.

- **DS4.9 Almacenamiento de respaldos fuera de las instalaciones:** se analizó las políticas de seguridad para copias de seguridad de la información del aplicativo INFO-SALUD que se implementan en la institución, esto con el objetivo de:

  - ✓ Mantener planes efectivos de seguridad de backup con el fin de garantizar la seguridad, integridad y confidencialidad de la información extraída de la aplicación informática INFO-SALUD.

  - ✓ Asegurar que la información permanezca integra y a la mano al momento de iniciar un proceso de reanudación de servicios, con el fin de lograr el mínimo nivel de afectación en los procesos de la institución al momento de falla en el aplicativo.

  Este objetivo de control se analizó mediante la aplicación de las siguientes actividades:

  - ✓ Se analizó las políticas y prácticas de seguridad de backups que se implementan en la IPSI con el fin de salvaguardar la información gestionada por el aplicativo INFO-SALUD.

  - ✓ Se realizó un análisis de riesgos de todo el proceso de backup del aplicativo informático INFO-SALUD.

- ✓ Evaluar si los protocolos de copias de seguridad son parte integral de la estrategia de la empresa para salvaguardar la información contenida en la aplicación informática.

- ✓ Se aplicó entrevistas al ingeniero encargado del área de informática con el fin de conocer el proceso de copias de seguridad, encargados de esta actividad, pasos a seguir y lugar en donde se almacena la información.

- **DS4.10 Revisión post reanudación:** una vez lograda una exitosa reanudación de las funciones de TI después de una suspensión en sus servicios, determinar si las directivas de TI han establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

El análisis de los objetivos de control pertenecientes al proceso DS4 se evidencia en la aplicación mediante

- ✓ Definición de fuentes de conocimiento DS4
- ✓ Cuestionario cuantitativo DS4
- ✓ Cuadro de hallazgos DS4 (1)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**DS5 Garantizar la seguridad de los sistemas**

- **DS5. 1 Administración de la seguridad TI:** todos los planes de administración deben ser generados y aprobados por las directivas de la institución, motivo por el cual el análisis de estos procedimientos no fueron analizados en esta auditoría, ya que está encaminada solo al funcionamiento del aplicativo INFO-SALUD.

- **DS5.2 Plan de seguridad de TI:** se evaluó si la entidad cuenta con un plan de seguridad enfocado a la información gestionada por el aplicativo informático INFO-SALUD, con el finalidad de:

  - ✓ Prevenir, proteger y resguardar la información administrada por el aplicativo informático previniendo así robo, alteración o divulgación de datos confidenciales y de gran importancia para la IPSI Guaitara.

  Esto objetivo de control se analizó mediante teniendo en cuenta las siguientes actividades:

- ✓ Se aplicaron entrevistas al ingeniero encargado del área de sistemas con el fin de evaluar la existencia de políticas de seguridad enfocadas a la protección de los archivos gestionados por el aplicativo informático INFO-SALUD.

- ✓ Mediante observación directa se analizaron los procedimientos de administración de identidad aplicados en el funcionamiento del aplicativo INFO-SALUD.
- ✓ Se aplicó entrevistas a los operarios encargados del manejo de los módulos del aplicativo con el fin de evaluar procedimientos de seguridad tenidos en cuenta durante su trabajo con el aplicativo.

- **DS5.3 Administración de identidad***:* se evaluó la existencia prácticas de seguridad donde se identifique el usuario que hace uso del aplicativo informático, esto con el fin de:

  - ✓ Definir la utilización personalizada de recursos y privilegios de acceso con el fin de proteger la integridad y la confidencialidad de la información gestionada por el aplicativo informático.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Se aplicó entrevistas al ingeniero encargado del área de sistemas de la institución con el fin de evaluar la existencia de un protocolo de seguridad que contenga la implementación de usuarios de acceso al aplicativo informático.

  - ✓ Se aplicó entrevistas a los operarios del aplicativo INFO-SALUD con el fin de analizar si se aplican los usuarios y contraseñas asignados por el área de sistemas para el ingreso a las funcionalidades de los módulos del aplicativo informático.

  - ✓ Se analizaron los niveles de seguridad de usuarios y contraseñas implementados.

  - ✓ Se analizó si los derechos de acceso se solicita mediante un proceso formal al ingeniero encargado de la administración de las cuentas de usuario del aplicativo informático.

- **DS5.4 Administración de cuentas de usuario**: se evaluó si existen procedimientos para la administración de permisos de acceso para las cuentas de usuario suministradas a los encargados del manejo de los módulos del aplicativo informático, esto con el fin de:

- ✓ Generar procesos que establezcan el momento de asignación de privilegios de acceso a cuentas y cierre o terminación de acceso, con el fin de salvaguardar la información de personal ajeno a la institución.

Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

- ✓ Análisis de procedimientos de asignación, modificación y cierre de cuentas de usuario y privilegios de acceso.

- ✓ Análisis de privilegios de acceso otorgados a los operarios del aplicativo informático, teniendo en cuenta sus funciones.

- ✓ Análisis de la existencia de procedimientos para realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

- **DS5.5 Pruebas, vigilancia y monitoreo de la seguridad:** este objetivo de control no fue tomado en cuenta para su análisis debido a que hace referencia a planes de seguridad implementados para toda la institución, y no se enfoca al estudio del aplicativo informático INFO-SALUD.

- **DS5.6 Definición de incidente de seguridad:** este objetivo de control no ha sido analizado en el desarrollo de este trabajo de grado ya que la definición de procesos de gestión de incidentes son desarrollados por la administración y los representantes de cada dependencia de la IPSI, por lo tanto no es de la competencia del software INFO-SALUD.

- **DS5.7 Protección de la tecnología de seguridad:** se analizó si se implementan mecanismos para la protección de la información gestionada en el aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Implementar protocolos que garanticen que el aplicativo sea resistente a ataques que puedan revelar datos confidenciales de los pacientes.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Verificación de resistencia de seguridad de la base de datos del aplicativo informático.

- ✓ Verificación si las configuraciones de red son resistentes a ataques de personal del exterior.

- ✓ Verificación de protocolos de seguridad que como niveles de seguridad de contraseñas son los adecuados para proteger la información almacenada en la base de datos del aplicativo informático INFO-SALUD.

- ✓ Verificación de políticas de entrenamiento al personal operario en temas de seguridad de información.

- **DS5.8 Administración de llaves criptográficas:** se verificó si existen protocolos para la protección de las contraseñas utilizadas por los operarios para el acceso a la información almacenada en el aplicativo informático INFO-SALUD, esto con el fin de:

  - ✓ Concientizar sobre la implantación de un plan de seguridad de acceso al aplicativo adecuado con el fin de proteger la información almacenada en la base de datos del aplicativo.

  Esto se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Se aplicaron entrevistas al ingeniero encargado del área de sistemas con fin de evaluar la existencia de protocolos de gestión de contraseñas para el acceso al aplicativo informático INFO-SALUD.

  - ✓ Análisis del contenido de un plan de gestión de contraseñas en el cual se debe tener en cuenta aspectos como: tamaño de la contraseña, periodicidad de cambio obligatorio de contraseñas, confidencialidad de la contraseña y nivel se seguridad de la contraseña.

  - ✓ Se aplicaron entrevistas a los operarios del aplicativo con el fin de evaluar el conocimiento de los operarios acerca de la seguridad de cuentas de usuario y confidencialidad de contraseñas.

- **DS5.9 Prevención, detección y corrección de software malicioso***:* se evaluó la existencia de medidas de prevención y corrección en cuanto a daños al aplicativo informático debido software malicioso, esto con la finalidad de:

  - ✓ Proteger la información y el funcionamiento de la aplicación de ataques de programas informáticos maliciosos que pueden

corromper o eliminar la información gestionada en el aplicativo informático.

Lo anterior se analizó teniendo en cuenta los siguientes aspectos:

- ✓ Se verificó la existencia de programas antivirus instalados en los equipos en donde se mantiene la aplicación informática INFO-SALUD.

- ✓ Analizar la existencia de planes de capacitación impartidos a los funcionarios encaminados a la prevención de daños ocasionados por software externo.

- ✓ Evaluar la existencia de procedimientos para el manejo y corrección de problemas ocasionados por software malicioso generalmente en el caso de virus.

- **DS5.10 Seguridad de la red:** este objetivo de control no fue tomado en cuenta ya que pertenece al análisis del todo el sistema de información de las sedes de la IPSI Guaitara.

El análisis de los objetivos de control pertenecientes al proceso DS5 se evidencia en la aplicación mediante

- ✓ Definición de fuentes de conocimiento DS5
- ✓ Cuestionario cuantitativo DS5
- ✓ Cuadro de hallazgos DS5 (1)
- ✓ Cuadro de hallazgos DS5 (2)
- ✓ Cuadro de hallazgos DS5 (3)
- ✓ Cuadro de hallazgos DS5 (4)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**DS6 Identificar y asignar costos**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**DS7 Educar y entrenar a los usuarios**

- **DS7.1 Identificación de necesidades de entrenamiento y educación***:* se analizó la existencia de un programa de entrenamiento para los operarios del aplicativo informático INFO-SALUD, esto con el objetivo de:

  - ✓ Instaurar planes de capacitación orientando a obtener un buen nivel de conocimientos y habilidades de los empleados encargados del manejo de los módulos del aplicativo informático.

  - ✓ Incrementar la productividad y la eficiencia de los operarios del aplicativo informático.

  Lo anterior se examinó mediante las siguientes actividades:

  - ✓ Se evaluó la existencia de programas de entrenamiento para empleados que tienen contacto directo con el aplicativo informático INFO-SALUD.

  - ✓ Se analizó la estructura del plan de entrenamiento en el cual se deben atender las necesidades de formación y entrenamiento apropiado para los empleados que se encargarán del manejo de los módulos del aplicativo INFO-SALUD.

  - ✓ Se verificó la existencia de manuales de usuario en donde se especifiquen instrucciones acerca del funcionamiento del aplicativo informático.

- **DS7.2 Impartición de entrenamiento y educación:** se evaluó si existen planes de entrenamiento formales con enfoque sistémico aplicado a las necesidades de la institución y operarios de los módulos del aplicativo INFO-SALUD, esto con el fin de:

  - ✓ Establecer de manera ordena las actividades que se deben seguir al momento de impartir la capacitación al personal encargado del aplicativo informático.

  Este objetivo de control se analizó teniendo mediante las siguientes actividades:

  - ✓ Se evaluó la estructura del plan de entrenamiento, enfocándose en condiciones clave como:

- Detección de necesidades de formación o adiestramiento y clasificar la prioridad de las mismas.

- Programación y organización de las actividades de entrenamiento.

- Métodos de instrucción.

- Tiempos necesarios.

- Definir instructores, para la parte práctica y para la teórica (si es necesario).

- Métodos para medir la eficacia del plan de entrenamiento

- **DS7.3 Evaluación del entrenamiento recibido:** se evaluó si existen políticas para medir estándares de calidad para medición de cumplimiento de estándares de calidad del plan de entrenamiento.

  Este objetivo se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Se analizó si existen prácticas para la evaluación de resultados con el fin de constatar si se ha alcanzado los objetivos fijados al inicio del programa de entrenamiento.

  - ✓ Se analizó la reacción del grupo capacitado, dudas e inquietudes de la capacitación recibida.

  - ✓ Se analizó la existencia de planes de medición de resultados obtenidos con la aplicación del plan de entrenamiento en cuanto a mejoras en eficiencia y eficacia en la operación de procesos en la aplicación informática INFO-SALUD.

El análisis de los objetivos de control pertenecientes al proceso DS7 se evidencia en la aplicación mediante

- ✓ Definición de fuentes de conocimiento DS7
- ✓ Cuestionario cuantitativo DS7
- ✓ Cuadro de hallazgos DS7 (1)
- ✓ Cuadro de valoración de riesgos
- ✓ Matriz de probabilidad e impacto

**DS8 Administrar la mesa de servicio y los incidentes**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD.

**DS9 Administrar la configuración**

Este dominio no fue tomado en cuenta ya que se refiere a configuraciones de hardware de TI que no se enfocan al funcionamiento del software INFO-SALUD.

**DS10 Administración de problemas**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia a procesos netamente administrativos y no se enfocan al funcionamiento del software INFO-SALUD

**DS11 Administración de datos**

Los objetivos de control pertenecientes a este proceso no fueron tomados en cuenta para el análisis de esta auditoría ya que hacen referencia políticas se seguridad de la organización y no se enfocan al funcionamiento del software INFO-SALUD

**DS12 Administración del ambiente físico**

- **DS12.1 Selección y diseño del centro de datos:** este objetivo de control no fue tomado en cuenta en la ejecución de esta auditoría dado que busca definir estrategias tecnológicas de tipo físico para el centro de Informática en general y la auditoría se enfocó al aplicativo informático INFO-SALUD que se encuentra alojado en un servidor.

- **DS.12.2 Medidas de seguridad física:** se verificó la existencia de protocolos de seguridad dirigidos a la seguridad física del servidor y de los equipos en donde se encuentra instalado aplicativo informático INFO-SALUD, esto con el fin de:

    - ✓ Garantizar la seguridad de la base de datos del aplicativo informático INFO-SALUD.

- ✓ Garantizar la continua prestación de servicios del aplicativo informático, tomando medidas de seguridad física en cada uno de los equipos.

Los aspectos a considerar en el análisis de este objetivo fueron:

- ✓ Se evaluó por medio de la aplicación de entrevistas al ingeniero encargado del área de sistemas la existencia de normatividad de seguridad física que proteja los equipos en donde se encuentra alojada la aplicación informática INFO-SALUD.

- ✓ Se revisó el cumplimiento de las medidas de seguridad física por parte del personal encargado del centro de cómputo de la IPSI GUAITARA.

- ✓ Verificación de la existencia de personal encargado del monitoreo de incidentes de seguridad física en el área del servidor en donde se encuentra alojada la aplicación informática INFO-SALUD.

- **DS12.3 Acceso físico:** se evaluó la existencia de procedimientos para controlar el acceso al centro de cómputo por personal no autorizado, esto con el fin de:

  Respaldar la seguridad del servidor en donde se encuentra alojada la aplicación informática INFO-SALUD, con el fin evitar daños en la base de datos del aplicativo.

  Este objetivo de control se analizó teniendo en cuenta los siguientes aspectos:

  - ✓ Mediante entrevistas con el ingeniero encargado se evaluó la existencia controles de acceso físico al centro de informática donde se encuentra el servidor de la aplicación informática INFO-SALUD.

  - ✓ Se analizó si en el protocolo de acceso al centro de informático se establecen medidas como justificación de acceso al centro, autorización, registro y monitoreo de la visita.

- **DS12.4 Protección contra factores ambientales:** este objetivo no fue tomado en cuenta durante el desarrollo de esta auditoría debido a que hace referencia al aspecto físico de la entidad en general más donde se encuentra el servidor del software INFO-SALUD.

- **DS12.5 Administración de instalaciones físicas:** este objetivo no fue tomado en cuenta durante el desarrollo de esta auditoría debido a que hace referencia al aspecto físico de la entidad en general más donde se encuentra el servidor del software INFO-SALUD.

**DS13 Administración de operaciones**

- **DS13.5 Mantenimiento preventivo del hardware**: se evaluó si existen procedimientos que establezcan actividades de mantenimiento preventivo a los equipos de cómputo donde se encuentra alojada la aplicación informática INFO-SALUD, esto con el fin de:

  - ✓ Reducir la frecuencia y el impacto de fallas de desempeño del aplicativo INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

  - ✓ Por medio de la aplicación de entrevistas al ingeniero encargado del centro de informática de la IPSI, se evaluó la existencia de planes de mantenimiento preventivo al hardware en donde se encuentra funcionando el aplicativo informático.

  - ✓ Se evaluó si el plan de mantenimiento cuenta con actividades como cronograma de mantenimiento, asignación de actividades, limpieza física del hardware, instalación de antivirus, formateo de equipos en caso de ser necesario, Actualización de programas y eliminación de archivos muertos.

**Dominio: monitorear y evaluar (ME)**

**ME2 Monitorear y evaluar el control interno**

- **ME2.3 Excepciones de control:** se evaluó la existencia de protocolos para analizar e identificar una variedad de vulnerabilidades que puedan afectar el correcto funcionamiento del aplicativo informático INFO-SALUD;
  esto con el fin de:

  - ✓ Establecer acciones correctivas necesarias con el fin de evitar errores e inconsistencias en los datos administrados por la aplicación informática INFO-SALUD.

  Este objetivo de control se analizó teniendo en cuenta las siguientes actividades:

- ✓ Se aplicaron entrevistas al ingeniero encargado del área de sistemas con el fin de evaluar la existencia de un marco de trabajo de control interno enfocado a la aplicación informática INFO-SALUD.

- ✓ Se analizó la política de mejoramiento con el fin de estableces acciones correctivas para garantizar el buen funcionamiento de la aplicación informática.

**3.2.3 Cuadros de definición de fuentes de conocimiento.** Para el desarrollo de la auditoría informática a los módulos HistoriaNet, Citas Médicas, Facturación y Kardex del software INFO-SALUD de la IPS Indígena Guaitara se realizaron entrevistas con los funcionarios de la IPS Indígena y el encargado del Centro de Informática, pruebas de análisis y de ejecución de los módulos del software con el fin de obtener mayor claridad en la eficiencia, eficacia e integridad de los datos, esto con el fin de identificar posibles riesgos y generar las respectivas alternativas de solución.

A continuación, se muestra los cuadros de fuentes de conocimiento aplicado en la IPSI Guaitara basándose en los dominios de COBIT.

**Dominio planeación y organización (PO)**

<table>
<tr><td rowspan="2">  </td><td colspan="3" rowspan="2">CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA</td><td colspan="3">REF</td></tr>
<tr><td colspan="3">PLAN PO2</td></tr>
<tr><td>ENTIDAD AUDITADA</td><td colspan="3">IPS INDÍGENA GUAITARA</td><td colspan="3">PÁGINA</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="3">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td><td>1</td><td>DE</td><td>1</td></tr>
<tr><td>RESPONSABLES</td><td colspan="6">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="6">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Planeación y organización (PO)</td><td>PROCESO</td><td colspan="4">PO2 Definir la Arquitectura de la Información.</td></tr>
<tr><td>DESCRIPCIÓN DE ACTIVIDAD/PRUEBA</td><td colspan="6">Evaluar la respuesta a los requerimientos y la salida de información confiable y consistente del Software.</td></tr>
<tr><td colspan="7"></td></tr>
<tr><td rowspan="2">FUENTES DE CONOCIMIENTO</td><td colspan="6">REPOSITORIO DE PRUEBAS APLICABLES</td></tr>
<tr><td colspan="3">DE ANÁLISIS</td><td colspan="3">DE EJECUCIÓN</td></tr>
<tr><td>✓ Entrevista al Ingeniero encargado del Centro de Informática.<br><br>✓ Encuestas y entrevistas a operarios de los módulos de cada dependencia.</td><td colspan="3">✓ Analizar entrevista al Ingeniero encargado del Centro de Informática<br><br>✓ Analizar entrevista de funcionarios de cada dependencia<br><br>✓ Analizar el funcionamiento de los módulos del software.<br><br>✓ Verificación de existencia de un modelo de información</td><td colspan="3">✓ Revisión del funcionamiento de los módulos del software INFO-SALUD<br><br>✓ Aplicación de pruebas y verificación de datos inconsistentes<br><br>✓ Obtención de elementos y datos redundantes / duplicados.</td></tr>
</table>

Cuadro 7. Definición de fuentes de conocimiento PO2. [1]

| | | | |
|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | | **REF** PLAN PO4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | **PÁGINA** **1** **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | PO4 Definir los procesos, organización y relaciones de TI |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar estructuras organizacionales, roles y responsabilidades para todos los procesos permitiendo el buen funcionamiento de servicios que satisfagan los objetivos de la institución. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara.<br><br>✓ Entrevista a los funcionarios de la IPS Indígena Guaitara.<br><br>✓ Descripción documentada de los roles y responsabilidades del personal.<br><br>✓ Descripción documentada de procedimientos | ✓ Analizar el manual de funciones del personal operario del software.<br><br>✓ Analizar los roles y responsabilidades del personal.<br><br>✓ Revisión detallada de funciones y procedimientos de la organización. | ✓ Análisis de responsabilidades según la asignación de roles.<br><br>✓ Comparación de funciones documentadas con las funciones realizadas por los trabajadores. |

Cuadro 8. Definición de fuentes de conocimiento PO4. [1]

| | | | | |
|---|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | | | **REF** PLAN PO7 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** **1** **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | PO7 Administrar los recursos humanos de TI | |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Examinar los procesos de contratación, entrenamiento del personal y asociación de roles que correspondientes a las habilidades de los individuos. | | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara<br>✓ Entrevista al ingeniero encargado del Centro de Informática.<br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br>✓ Documentación entregada por el personal. | ✓ Observación de desempeño del personal.<br>✓ Análisis de entrenamiento del personal operario de los módulos de INFO-SALUD.<br>✓ Análisis sobre alta rotación de empleados.<br>✓ Análisis de documentación existente enfocada a la capacitación de personal. | ✓ Desarrollo y Evaluación de resultados de Ratio de rotación de personal TI<br>✓ Comparación de material de ayuda para entrenamiento vs Software.<br>✓ Verificación de procesos de captura conocimiento (documentación).<br>✓ Verificación número promedio de días de entrenamiento (funcionamiento de módulos). |

Cuadro 9. Definición de fuentes de conocimiento PO7. [1]

| | | | | |
|---|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | | | **REF** PLAN PO9 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | PO9. Evaluar y Administrar los Riesgos de TI | |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Análisis del marco de trabajo de administración de riesgos dirigido al funcionamiento del software INFO-SALUD. | | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas a los operarios de los módulos de software. | ✓ Análisis de eventos de respuesta a riesgos.<br><br>✓ Análisis de procesos de respuesta a riesgos.<br><br>✓ Análisis de tiempos de respuesta a fallos. | ✓ Evaluar la existencia de documentación de riesgos y actividades de control<br><br>✓ Aplicación de entrevistas a los operarios de los módulos del software, con el fin de analizar sus habilidades, uso, acceso y responsabilidades. |

Cuadro 10. Definición de fuentes de conocimiento PO9. [1]

**Dominio adquirir e implementar (AI)**

<table>
<tr><td rowspan="2"></td><td colspan="3" rowspan="2">CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA</td><td>REF</td></tr>
<tr><td>PLAN AI1</td></tr>
<tr><td>ENTIDAD AUDITADA</td><td colspan="3">IPS INDÍGENA GUAITARA</td><td>PÁGINA<br>1 DE 1</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="4">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="4">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="4">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Adquirir e implementar (AI).</td><td>PROCESO</td><td colspan="2">AI1 Adquirir e Implementar</td></tr>
<tr><td>DESCRIPCIÓN DE ACTIVIDAD/PRUEBA</td><td colspan="4">Analizar los requerimientos de negocio funcional y técnico que se tuvieron en cuenta para la adquisición del software.</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td rowspan="2">FUENTES DE CONOCIMIENTO</td><td colspan="4">REPOSITORIO DE PRUEBAS APLICABLES</td></tr>
<tr><td colspan="2">DE ANÁLISIS</td><td colspan="2">DE EJECUCIÓN</td></tr>
<tr><td>✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara.<br><br>✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.</td><td colspan="2">✓ Análisis de aprobación de requerimientos y proceso de adquisición del software INFO-SALUD.<br><br>✓ Analizar el funcionamiento de los módulos del software.<br><br>✓ Analizar la existencia de un estudio de factibilidad del software.</td><td colspan="2">✓ Aplicación de pruebas de aceptación de requerimientos al software con el fin de evaluar el cumplimiento de las necesidades de la IPSI.</td></tr>
</table>

Cuadro 11. Definición de fuentes de conocimiento AI1. [1]

| | | |
|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | **REF** PLAN AI2 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** **1** **DE** **1** |

| | | | |
|---|---|---|---|
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | AI2 Identificar Soluciones Automatizadas |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evidenciar que la funcionalidad del software se desarrolle de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Documentación entregada por el personal administrativo. | ✓ Analizar si la participación de los operarios del software es significativa.<br><br>✓ Analizar si hay un proceso apropiado para el diseño del sistema, teniendo en cuenta entrada, procedimiento y salida de datos.<br><br>✓ Analizar si existe un plan de pruebas del proyecto y un proceso de aprobación de usuario.<br><br>✓ Revisión detallada de documentación para evaluar el cumplimiento de los requerimientos | ✓ Comparación entre documentos de requerimientos con funcionalidad del software.<br><br>✓ Revisar en el módulo si las especificaciones usuario-maquina son fáciles de usar para los operarios del software.<br><br>✓ Aplicación de entrevistas para una revisión detallada de la satisfacción del usuario con el modulo. |

Cuadro 12. Definición de fuentes de conocimiento AI2. [1]

| | | | | |
|---|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | | | **REF** PLAN AI4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** **1** **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | AI4 Facilitar la Operación y el Uso | |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar la existencia de documentación y manuales efectivos de usuario y de operación así como el respectivo material de entrenamiento que permita transferir el conocimiento necesario para la correcta operación de los módulos del software. | | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Documentación entregada por el personal administrativo. | ✓ Analizar metodología de transferencia de conocimiento.<br><br>✓ Evaluar la existencia de documentación de soporte de transferencia de conocimiento.<br><br>✓ Analizar manuales de procedimientos del usuario final.<br><br>✓ Evaluar la existencia de documentación de soporte técnica para operaciones y personal de soporte encargado de la manipulación de los módulos del software. | ✓ Aplicación de entrevistas para evaluar satisfacción de planes de entrenamiento y documentación.<br><br>✓ Aplicación de entrevistas para evaluar existencia y aplicación de planes de transferencia de conocimiento. |

Cuadro 13. Definición de fuentes de conocimiento AI4. [1]

| | | |
|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | **REF** PLAN AI6 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** **1 DE 1** |

| | | | |
|---|---|---|---|
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | AI6 Administrar cambios |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar los planes para la administración formal y controlada de actualizaciones y mantenimiento para el software INFO-SALUD. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara.<br><br>✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Documentación entregada por el personal administrativo. | ✓ Analizar si existe un proceso para realizar cambios para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio.<br><br>✓ Analizar si existe reportes de cambios de T.I<br><br>✓ Analizar si existen manuales con los nuevos cambios implementados en el software. | ✓ Constatar porcentaje de cambios en el software (actualizaciones) que siguen procesos de control de cambio formales.<br><br>✓ Inspeccionar mediante entrevistas si los usuarios están satisfechos con el resultado de los cambios solicitados |

Cuadro 14. Definición de fuentes de conocimiento AI6. [1]

| | | | |
|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA** | | **REF** PLAN AI7 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | **PÁGINA** **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | AI7 Instalar y Acreditar Soluciones y Cambios |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar que el software y sus actualizaciones trabajen sin problemas importantes después de la instalación. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil. | ✓ Análisis de planes de entrenamiento al personal de los departamentos de acuerdo con la metodología de implementación.<br><br>✓ Análisis de participación de funcionarios encargados del manejo de los módulos pertenecientes a INFO-SALUD y evaluar si se tomó en cuenta sus aportes durante el periodo de prueba del software<br><br>✓ Análisis de existencia de plan de implantación formal donde se definan las tareas o agenda de implantación del aplicativo informático. | ✓ Aplicación de entrevistas con fin de evaluar controles internos, practicas operativas, calidad de datos y cargas de trabajo por parte de los operarios.<br><br>✓ Entrevista con el ingeniero con fin de determinar número de llamadas de usuarios después de la actualización debido a capacitación . |

Cuadro 15. Definición de fuentes de conocimiento AI7. [1]

**Dominio entregar y dar soporte (DS)**

| | | | |
|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | | **REF** PLAN DS3 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | **PÁGINA** 1 **DE** 1 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS3 Administrar el desempeño y la capacidad |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar el desempeño y la capacidad del software en respuesta a las necesidades de la entidad. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br>✓ Módulos del software INFO-SALUD.<br>✓ Sistema Gestor de base de datos. | ✓ Evaluar el sistema de administración de base de datos que permiten la gestión de la información en la entidad.<br>✓ Revisar el desempeño y capacidad actual de los recursos de TI.<br>✓ Monitorear el desempeño y capacidad de los recursos del sistema gestor de base de datos. | ✓ Evaluar que sistema gestor de base de datos es utilizado por el software INFO-SALUD.<br>✓ Examinación directa del software y su gestor de base de datos para conocer características y capacidades.<br>✓ Aplicación de entrevistas con el fin de documentar la confiabilidad. |

Cuadro 16. Definición de fuentes de conocimiento DS3. [1]

| | | | | |
|---|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | | | **REF** PLAN DS4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS4 Garantizar la Continuidad del | |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar que el software y sus actualizaciones trabajen sin problemas importantes después de la instalación. | | | |
| | | | | |
| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | | | |
| | **DE ANÁLISIS** | | **DE EJECUCIÓN** | |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Módulos del software INFO-SALUD. | ✓ Evaluar la existencia de un plan de continuidad activo, vigente y actualizado<br><br>✓ Análisis de planes de continuidad TI y sus niveles de prioridad.<br><br>✓ Análisis de metodología de entrenamiento a los funcionarios.<br><br>✓ Análisis de pruebas realizados a los planes de contingencia TI.<br><br>✓ Evaluar la existencia de copias de seguridad de los datos fuera de las instalaciones.<br><br>✓ Análisis de procedimientos Post-reanudación. | | ✓ Aplicación de entrevistas con el fin de evaluar Procesos críticos de la entidad que dependen del software<br><br>✓ Comprobación del funcionamiento de los procesos dependientes de los módulos de historiaNet, citas médicas, facturación y kardex del software.<br><br>✓ Solicitud de registros para comprobar consistencia en datos. | |

Cuadro 17. Definición de fuentes de conocimiento DS4. [1]

| | | |
|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | **REF** PLAN DS5 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** **1 DE 1** |

| | | | |
|---|---|---|---|
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS5 Garantizar la Seguridad de los Sistemas |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Analizar los procesos de administración de seguridad que permitan mantener la integridad de la información y la protección de los datos. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Módulos del software INFO-SALUD.<br><br>✓ Instalaciones físicas de la dependencia | ✓ Evaluar la existencia de políticas de seguridad TI.<br><br>✓ Comprobar existencia de procesos de administración de identidad (cuentas).<br><br>✓ Análisis de procedimientos para monitorear incidentes de seguridad, reales y potenciales.<br><br>✓ Análisis de procedimientos para el manejo y corrección de problemas ocasionados por software malicioso generalmente en el caso de virus. | ✓ Mediante observación directa y verificación del software analizar el control de acceso.<br><br>✓ Mediante observación directa y verificación del software revisión de privilegios y derechos de acceso de los usuarios.<br><br>✓ Verificación en el software de niveles de seguridad. |

Cuadro 18. Definición de fuentes de conocimiento DS5. [1]

| | | |
|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | **REF** PLAN DS7 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** **1 DE 1** |

| | | | |
|---|---|---|---|
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS7 Educar y Entrenar a los Usuarios |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología realizando un plan completo de entrenamiento y desarrollo. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara.<br>✓ Entrevista al ingeniero encargado del Centro de Informática.<br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil. | ✓ Evaluar la existencia de programas de entrenamiento para empleados que tienen contacto directo con el software.<br>✓ Análisis de actualización de los planes de entrenamiento de forma regular<br>✓ Análisis de estrategias para monitorear y reportar la efectividad del entrenamiento. | ✓ Mediante observación directa y encuestas evaluar efectividad de los panes de entrenamiento.<br>✓ Aplicación de pruebas cuantitativas del porcentaje de satisfacción de operarios con el plan de entrenamiento recibido. |

Cuadro 19. Definición de fuentes de conocimiento DS7. [1]

| | | | |
|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | | **REF** PLAN DS12 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | **PÁGINA** **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS12 Administración de Ambiente Físico. |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Evaluar la protección de los activos de cómputo y la información de la entidad minimizando el riesgo de una interrupción del servicio por fallas del hardware en la Institución. | | |
| | | | |
| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | | |
| | **DE ANÁLISIS** | | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Visita a instalaciones físicas. | ✓ Evaluar existencia de procesos para la seguridad física de los activos de TI.<br><br>✓ Evaluar el control de acceso a áreas de TI (servidor y centro de cómputo)<br><br>✓ Evaluar si el equipo de comunicaciones, suministro de energía y red trabajan según las especificaciones técnicas de la empresa. | | ✓ Evaluar mediante observación directa la efectividad de los procedimientos para mantener un ambiente físico adecuado para la infraestructura TI.<br><br>✓ Mediante observación directa estimar si los controles de seguridad son suficientes de acuerdo a las necesidades de la empresa. |

Cuadro 20. Definición de fuentes de conocimiento DS12. [1]

| | | | |
|---|---|---|---|
| | **CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN** | | **REF** PLAN DS13 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | **PÁGINA** **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | DS13 Administración de Operaciones. |
| **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA** | Analizar la efectividad en la administración y protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware en la Institución. | | |

| **FUENTES DE CONOCIMIENTO** | **REPOSITORIO DE PRUEBAS APLICABLES** | |
|---|---|---|
| | **DE ANÁLISIS** | **DE EJECUCIÓN** |
| ✓ Entrevista al ingeniero encargado del Centro de Informática.<br><br>✓ Entrevistas y encuestas realizadas a los funcionarios según su perfil.<br><br>✓ Manual de funciones | ✓ Análisis de procedimientos para garantizar el mantenimiento oportuno de la infraestructura y el software INFO-SALUD.<br><br>✓ Evaluar existencia de un plan de soporte técnico.<br><br>✓ Evaluar políticas y procedimientos de operación de protección de datos de salida, monitoreo de infraestructura y mantenimiento preventivo del hardware. | ✓ Aplicación de entrevista al ingeniero encargado para comprobar frecuencia con que se realiza mantenimiento preventivo a los equipos de las dependencias.<br><br>✓ Mediante entrevista con el ingeniero encargado evaluar con qué frecuencia el centro de informática realiza revisiones en el software INFO-SALUD. |

Cuadro 21. Definición de fuentes de conocimiento DS13. [1]

**Dominio entregar y dar soporte (ME)**

<table>
<tr><td rowspan="2"></td><td colspan="3" rowspan="2">CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE EJECUCIÓN</td><td>REF</td></tr>
<tr><td>PLAN ME2</td></tr>
<tr><td>ENTIDAD AUDITADA</td><td colspan="3">IPS INDÍGENA GUAITARA</td><td>PÁGINA<br>1 DE 1</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="4">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="4">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="4">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Monitorear Y Evaluar (ME).</td><td>PROCESO</td><td colspan="2">ME2 Excepciones de Control</td></tr>
<tr><td>DESCRIPCIÓN DE ACTIVIDAD/PRUEBA</td><td colspan="4">Analizar la existencia de procesos de monitoreo de control interno TI garantizando el logro de los objetivos de la institución.</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td rowspan="2">FUENTES DE CONOCIMIENTO</td><td colspan="4">REPOSITORIO DE PRUEBAS APLICABLES</td></tr>
<tr><td colspan="2">DE ANÁLISIS</td><td colspan="2">DE EJECUCIÓN</td></tr>
<tr><td>✓ Entrevista al personal Administrativo de la IPS Indígena Guaitara.<br><br>✓ Entrevista al ingeniero encargado del Centro de Informática.</td><td colspan="2">✓ Evaluar existencia de un marco de trabajo de controles internos TI.<br><br>✓ Verificación de procesos de auto-evaluación.<br><br>✓ Análisis de planes de mejoramiento.</td><td colspan="2">✓ Análisis de acciones correctivas teniendo en cuenta los procesos de control interno.</td></tr>
</table>

Cuadro 22. Definición de fuentes de conocimiento ME2. [1]

Para observar la totalidad de los cuadros de definición de fuentes de conocimiento utilizados en el desarrollo de la auditoría, ver **ANEXO B. Dominio, planeación y organización,** de manera digital en la carpeta:

Evidencias\ANEXO B. Dominio, planeación y organización \ Dominio, planeación y organización.docx

**3.2.4 Cuestionarios cuantitativos.** Los cuestionarios cuantitativos permiten definir preguntas tomando como base el cuadro de definición de fuente de conocimiento.

Enseguida se muestran los cuestionarios cuantitativos aplicados en los procesos analizados para esta auditoría.

| | | | | |
|---|---|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | | | **REF** PLAN PO2 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** 1 DE 1 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | PO2 Definir la Arquitectura de la Información. | |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. Existe un documento donde se especifique un modelo de datos donde se describa el tipo de los datos que hay en la base y la forma en que se relacionan. | | **3** | | |
| 2. Existe un manual de diseño del software donde se especifiquen: | | | | |
| • ¿Requerimientos del software y hardware para su funcionamiento? | | **4** | | |
| • ¿Descripción de la configuración? | **3** | | | |
| • ¿Descripción de operación de cada botón y elementos del módulo? | | **2** | | |

| | | | | |
|---|---|---|---|---|
| • ¿Diagramas de flujo de datos o pseudocódigo de las partes del módulo? | | **3** | | |
| • ¿Lista de archivos y especificaciones? | | | | |
| 3. ¿Existe el diccionario de datos donde se especifiquen los datos que se manejan en el software? | | **4** | | |
| 4. El diccionario de datos contiene: | | **4** | | |
| • ¿Tablas? | | | | |
| • ¿Relaciones? | | | | |
| • ¿Llaves? | | | | |
| • ¿Descripción del personal encargado de la función de dar mantenimiento del diccionario de datos? | **4** | **4** | | |
| 5. ¿Le ha sido entregado al ingeniero encargado del centro de informática el diccionario de datos? | | **4** | | |
| 6. ¿Se ha establecido un procedimiento para mantener actualizado el diccionario de datos? | | **4**<br>**4** | | |
| 7. ¿Existen políticas y procedimientos en relación al modelo de arquitectura de información? | | **3** | | |
| 8. El modelo de arquitectura de información tiene en cuenta | | | | |
| • ¿Identificación de entrada? | **4** | | | |
| • ¿Identificación de procesos? | **4** | | | |
| • ¿Identificación de sitios de almacenamiento (base de datos)? | **4** | | | |

| | | | | |
|---|---|---|---|---|
| • ¿Identificación de reportes? | **4** | | | |
| • ¿Requerimientos para cada módulo? | **3** | | | |
| 9. ¿Existen esquemas donde se definan los niveles y controles apropiados de seguridad como controles de acceso? | **4** | | | |
| 10. ¿El personal aplica estos procedimientos de seguridad? | | **4** | | |
| 11. ¿El modelo de arquitectura de información ha sido entregado al personal del área de sistemas? | | **4** | | |
| **TOTAL** | **30** | **51** | | |
| **TOTAL CUESTIONARIO** | **81** | | | |

Cuadro 23. Cuestionario cuantitativo PO2. [1]

Porcentaje de Riesgo = (30*100)/(81-0) =37%
Porcentaje Riesgo total = 100-37%=63%(Riesgo Medio)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN PO4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | | PO4 Definir los procesos, organización |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. ¿Están claramente definidas las funciones que debe desempeñar el trabajador? | **4** | | | |
| 2. ¿Existe un manual de funciones donde se encuentre la definición y descripción? | **4** | | | |
| 3. ¿Se han implementado prácticas de supervisión y evaluación a los operadores del software para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada? | | **4** | | Existe dependencia hacia el ingeniero ya que es el único encargado de dar soporte al software. |
| 4. ¿Existen planes que eviten dependencia hacia el personal clave que desempeña funciones de trabajo críticas? | | **4** | | |
| 5. ¿En la entidad existen políticas y procedimientos para realizar la contratación de nuevo personal? | **3** | | | |
| 6. ¿Existen políticas para garantizar la protección de la información manejada por el personal operario? | **4** | | | |
| **TOTAL** | **15** | **48** | | |
| **TOTAL CUESTIONARIO** | **23** | | | |

Cuadro 24. Cuestionario cuantitativo PO4. [1]

Porcentaje de Riesgo = (15*100)/(23-0) =65%
Porcentaje Riesgo total = 100-65%=35%(Riesgo Bajo)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN PO7 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** | PO7 Administrar los recursos | |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. ¿Existen políticas de reclutamiento de personal? | **3** | | | |
| 2. ¿Existen políticas de retención de personal? | | **4** | | |
| 3. ¿Existen políticas para evaluar de forma periódica habilidades del personal para cumplir con sus funciones? | | **4** | | |
| 4. ¿Existen procesos de orientación continua del personal? | | **4** | | |
| 5. ¿Existen procedimientos para documentar el conocimiento de personal clave con el fin de evitar dependencia hacia personal clave? | | **3** | | |
| 6. ¿Existen procedimientos de documentación de control y registro? | | **4** | | |
| **7.** ¿Cuándo se presenta terminación de contrato del personal, existen políticas para eliminar privilegios de acceso? | | **4** | | |
| **TOTAL** | **3** | **23** | | |
| **TOTAL CUESTIONARIO** | **26** | | | |

Cuadro 25. Cuestionario cuantitativo PO7. [1]

Porcentaje de Riesgo = (3*100)/(26-0) =11,53%
Porcentaje Riesgo total = 100-11,53%=88,46%(Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | REF |
|---|---|---|
| | | PLAN PO9 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** **1** **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | |
| **MATERIAL DE SOPORTE** | COBIT | |
| **DOMINIO** | Planeación y organización (PO) | **PROCESO** PO9. Evaluar y Administrar los Riesgos de TI |

| PREGUNTAS | SI | NO | NA | OBSERVACIÓN |
|---|---|---|---|---|
| 1. Están identificadas amenazas físicas que podrían afectar el funcionamiento del software tales como: | | | | |
| • Incendios | | **3** | | |
| • robos | **3** | | | |
| • terrorismo | | **3** | | |
| • personal inconforme | | **3** | | |
| 2. ¿En la entidad existe una evaluación de riesgos del software que se encuentre plasmada en políticas o procedimientos? | | **4** | | |
| 3. ¿Se identifica con claridad las responsabilidades en cuanto al uso del sistema de información? | **3** | | | |
| 4. ¿Están documentados los procedimientos para la evaluación de riesgos lógicos? | | **4** | | |
| 5. ¿Dentro de este documento para la evaluación de riesgos se incluyen aspectos relacionados con la actualización o mantenimiento del hardware? | | **3** | | |
| 6. ¿Dentro del documento para la evaluación | | | | |

| | | | | |
|---|---|---|---|---|
| de riesgos se incluyen aspectos relacionados con el manejo que el usuario le da al equipo de trabajo, sus recursos de software e instalaciones de otros programas que quitan rendimiento al hardware o pueden ser causantes de adquisición de virus? | **4** | | | |
| 7. ¿En la entidad hay una medición de riesgos y amenazas que permitan cuantificar y cualificar cada uno de ellos? | | **4** | | |
| 8. ¿Se han organizado los riesgos de los módulos del software INFO-SALUD de acuerdo a su nivel de importancia e impacto? | | **4** | | |
| 9. ¿El plan de acción contra riesgos incluye seguimiento y monitoreo realizado al proceso? | | **4** | | |
| 10. ¿A los empleados, se ha realizado un proceso informativo y de toma de conciencia de la evaluación de riesgos? | | **4** | | El plan de mitigación consiste en llevar los registros en Excel o en Word. |
| 11. ¿Existen equipos de respaldo (super numerario) que garanticen la continuidad del servicio cuando se presente una falla en un equipo? | **4** | | | |
| 12. ¿Existen planes de mitigación de riesgos cuando se presentan fallas en el software INFO-SALUD con el fin de continuar con la prestación de servicio de salud en la entidad? | **4** | | | |
| 13. ¿Se considera estos planes de mitigación efectivos? | | **4** | | |
| **TOTAL** | **18** | **44** | | |
| **TOTAL CUESTIONARIO** | **62** | | | |

Cuadro 26. Cuestionario cuantitativo PO9. [1]

Porcentaje de Riesgo = (18*100)/(62-0) =29,03%
Porcentaje Riesgo total = 100-30%=71%(Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN AI1 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | | AI1 Identificar Soluciones Automatizadas |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. ¿Existen procedimientos para especificar y acordar los requerimientos funcionales y técnicos que cubran todas las necesidades de la organización? | | **4** | | |
| 2. ¿El Software cumple con los objetivos institucionales de la organización? | **4** | | | |
| 3. ¿El software se adapta a la razón de ser de la organización, en este caso una institución prestadora de servicios de salud de I nivel? | | **4** | | |
| 4. ¿Se desarrolló un estudio de factibilidad antes de la adquisición del software? | | **4** | | |
| **5.** ¿Se encuentra satisfecho con la funcionalidad del software? | | **4** | | |
| **TOTAL** | **4** | **16** | | |
| **TOTAL CUESTIONARIO** | **20** | | | |

Cuadro 27. Cuestionario cuantitativo AI1. [1]

Porcentaje de Riesgo = (4*100)/(20-0) =20%
Porcentaje Riesgo total = 100-20%=80%(Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN AI2 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | | AI2 Adquirir y Mantener |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. Existió un proceso gestión de requerimientos para la adquisición del software INFO SALUD | | | | |
| • Seguridad de la aplicación | | **4** | | |
| • Arquitectura de información | | **4** | | |
| • Tolerancia a riesgos | | **4** | | |
| 2. ¿El software se adapta a la razón de ser de la organización, en este caso un institución prestadora de servicios de salud de I nivel? | **4** | | | |
| 3. ¿Existe un proceso para el desarrollo de cambios importantes en la funcionalidad? | | **4** | | |
| 4. ¿Existe documentación donde se especifican datos de entrada y salida? | | **4** | | |
| 5. ¿Los diseños de los módulos de INFO-SALUD fueron aprobados por los operarios? | **4** | | | Los diseños se aprobaron en el año 2010 con la adquisición del software. |
| 6. ¿Existen planes de calidad de software con el fin de evaluar el cumplimiento de los requerimientos, políticas y procedimientos? | | **4** | | |
| 7. ¿Hay planes de mantenimiento de aplicación? | | **4** | | |
| **TOTAL** | **8** | **28** | | |
| **TOTAL CUESTIONARIO** | **36** | | | |

Cuadro 28. Cuestionario cuantitativo AI2. [1]

Porcentaje de Riesgo = (8*100)/(36-0) =22%
Porcentaje Riesgo total = 100-22%= 78%(Riesgo Alto)

| | | | | | |
|---|---|---|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | | | | **REF** PLAN AI4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | | **PÁGINA** 1 DE 1 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | | | AI4 Facilitar la Operación y el Uso |
| **PREGUNTAS** | | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
| 1. ¿Se desarrollan planes de capacitación inicial y a las personas encargadas del manejo de los módulos del software? | | **4** | | | La capacitación inicial se realizó en el 2010 fecha en la q se implanto el software |
| 2. ¿Estos planes de capacitación se realiza de manera continua? | | | **4** | | |
| 3. ¿Existe material de entrenamiento para el manejo del software INFO-SALUD manual de usuarios, manual de procedimientos? | | | **4** | | |
| 4. ¿Son suficientes los planes de entrenamiento ofrecidos a los operarios de los módulos de INFO-SALUD? | | | **4** | | |
| **TOTAL** | | **4** | **12** | | |
| **TOTAL CUESTIONARIO** | | **16** | | | |

Cuadro 29. Cuestionario cuantitativo AI4. [1]

Porcentaje de Riesgo = (4*100)/(16-0) =25%
Porcentaje Riesgo total = 100-25%=75% (Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN AI6 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Adquirir e implementar (AI). | PROCESO | AI6 Administrar cambios | |

| PREGUNTAS | SI | NO | NA | OBSERVACIÓN |
|---|---|---|---|---|
| 1. ¿Se lleva una documentación en bitácoras del monitoreo del proceso de cambios en el software? | | **3** | | |
| 2. ¿Para la realización de un cambio se lleva a cabo un proceso de solicitud y especificación del cambio? | **3** | | | |
| 3. ¿Se realizan pruebas de aceptación de la actualización? | | **3** | | |
| 4. ¿Se realiza un proceso de capacitación a los usuarios finales sobre el manejo del cambio en algún módulo? | | **3** | | |
| 5. ¿Se lleva un registro de los cambios realizados? | | **3** | | |
| 6. ¿Los manuales de los módulos se cambian cada vez que realizan actualizaciones? | | **3** | | |
| **TOTAL** | **3** | **15** | | |
| **TOTAL CUESTIONARIO** | **18** | | | |

Cuadro 30. Cuestionario cuantitativo AI6. [1]

Porcentaje de Riesgo = (3*100)/(18-0) =17%
Porcentaje Riesgo total = 100-17%=83%(Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN AI7 |
| ENTIDAD AUDITADA | IPS INDÍGENA GUAITARA | | | PÁGINA |
| | | | | 1 DE 1 |
| OBJETO DE ESTUDIO | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| RESPONSABLES | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| MATERIAL DE SOPORTE | COBIT | | | |
| DOMINIO | Adquirir e implementar (AI). | PROCESO | | AI7 Instalar y Acreditar Soluciones |

| PREGUNTAS | SI | NO | NA | OBSERVACIÓN |
|---|---|---|---|---|
| 1. ¿Existió un plan de pruebas basado en roles, responsabilidades y criterios de entrada y salida de información? | 4 | | | |
| 2. ¿Existen planes de entrenamiento al personal de los departamentos y al grupo de operaciones de acuerdo con los planes de implementación? | | 4 | | |
| 3. ¿Se estableció un entorno seguro de pruebas con el fin de evaluar funcionalidad del software? | | 4 | | |
| 4. ¿Se evaluaron si el software cumple con los niveles de seguridad, controles internos, prácticas operativas, calidad de datos y cargas de trabajo? | | 4 | | |
| 5. ¿Existen documentos de aceptación final después de haber realizado la evaluación de requerimientos? | 4 | | | |
| **TOTAL** | **8** | **12** | | |
| **TOTAL CUESTIONARIO** | **20** | | | |

Cuadro 31. Cuestionario cuantitativo AI7. [1]

Porcentaje de Riesgo = (8*100)/(20-0) =40%
Porcentaje Riesgo total = 100-40%=60% (Riesgo Medio)

| | CUESTIONARIO CUANTITATIVO | | | | REF PLAN DS3 |
|---|---|---|---|---|---|
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | | **PÁGINA 1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | Entregar y dar soporte (DS). | PROCESO | | | DS4 Garantizar la Continuidad del Servicio |
| **PREGUNTAS** | | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
| 1. ¿Se han detectado errores en el software por fallas en la capacidad de almacenamiento de la base de datos? | | **3** | | | El desarrollador es el único que conoce con exactitud los errores y soluciones de la base de datos. |
| 2. ¿Se ha dado seguimiento a las fallas? | | | **5** | | |
| 3. ¿Existen planes de contingencia para garantizar la continuidad del servicio cuando hay una falla en la base de datos? | | | **5** | | |
| 4. ¿Existe una base de datos de respaldo cuando la base de datos del servidor falla? | | | **4** | | |
| 5. Se monitorea de forma continua, compara y mejora el ambiente de funcionamiento control en cuanto: | | | | | |
| • Servidor | | **2** | | | |
| • Base de datos | | | **3** | | |
| 6. ¿Se tiene una bitácora de errores del sistema por fallas en el sistema gestor de base de datos? | | | **4** | | |
| 7. ¿Se conoce el límite de capacidad de almacenamiento del sistema gestor de | | **2** | | | |

| | | | | |
|---|---|---|---|---|
| base de datos?<br><br>8. ¿Se hace una revisión periódica de la capacidad y desempeño actual de la base de datos?<br><br>9. ¿Se tiene un pronóstico de capacidad de registros que pueden ser almacenados en la base de datos actual?<br><br>10. ¿Se evalúa la calidad de la información en la base de datos?<br><br>11. ¿Existen fallos en la base de datos cuando hay muchos equipos utilizando el software INFO-SALUD? | **4** | **5**<br><br>**4**<br><br>**4** | | |
| **TOTAL** | **11** | **34** | | |
| **TOTAL CUESTIONARIO** | **45** | | | |

Cuadro 32. Cuestionario cuantitativo DS3. [1]

Porcentaje de Riesgo = (11*100)/(45-0) =24%
Porcentaje Riesgo total = 100-24%=76%(Riesgo Alto)

| | | | | | |
|---|---|---|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | | | | **REF** PLAN DS4 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | | **PÁGINA** **1** **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | Entregar y dar soporte (DS). | PROCESO | | | DS4 Garantizar la Continuidad del Servicio |
| **PREGUNTAS** | | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
| 1. ¿En la entidad hay políticas y estrategias que garanticen la continuidad del servicio si se presentan fallas en el software?<br><br>2. ¿Considera que el plan de continuidad es | | **4** | | | |

| | | | | |
|---|---|---|---|---|
| acertado según las necesidades de información? | | **4** | | |
| 3. ¿Se lleva a cabo sesiones de entrenamiento con la frecuencia debida con respecto a lo que se debe realizar en caso de incidentes o interrupción no planeada? | **4** | | | |
| 4. ¿Los empleados tienen conocimiento de riesgos o situaciones que puedan interrumpir los procesos? | | **4** | | |
| 5. ¿Existe documentación o registro de las distintas interrupciones no planeadas en el software? | | **4** | | |
| 6. ¿Se lleva un control evaluando y verificando la precisión y eficiencia del plan? | | **4** | | |
| 7. ¿Se realiza un análisis de mejoramiento del plan de continuidad? | | **4** | | |
| 8. ¿Cómo plan de Continuidad se cuenta además con un respaldo de almacenamiento de información? | **4** | | | |
| 9. ¿Se almacena fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI? | | **5** | | |
| 10. ¿Existen planes para reanudación de las funciones después de una suspensión en sus servicios? | **4** | | | |
| **TOTAL** | **16** | **25** | | |
| **TOTAL CUESTIONARIO** | **41** | | | |

Cuadro 33. Cuestionario cuantitativo DS4. [1]

Porcentaje de Riesgo = (16*100)/(41-0) =39%
Porcentaje Riesgo total = 100-39%=61%(Riesgo Medio)

| | | |
|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | **REF** PLAN DS5 |
| **ENTIDAD AUDITADA** | **IPS indígena GUAITARA** | **PÁGINA** 1 **DE** 1 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | |
| **MATERIAL DE SOPORTE** | COBIT | |

| | | | |
|---|---|---|---|
| **DOMINIO** | Entregar y dar soporte (DS). | PROCESO | DS5 Garantizar la Seguridad de los Sistemas |

| **PREGUNTAS** | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
|---|---|---|---|---|
| 1. ¿En la entidad existe un plan de seguridad para la protección de la información? | | **4** | | |
| 2. ¿Tiene cada usuario su propia contraseña? | **4** | | | |
| 3. ¿Se exige periódicamente el cambio de contraseña? | | **4** | | |
| 4. ¿Existe un plan de seguridad que garantice la protección de los dispositivos y recursos de las dependencias? | **4** | | | |
| 5. ¿Los planes de seguridad son entregados a los operarios? | | **4** | | |
| 6. ¿Los operarios de los módulos de INF-SALUD ponen en práctica los planes de seguridad? | | **4** | | |
| 7. ¿En la entidad se encuentran asegurados físicamente los servidores? | **4** | | | |
| 8. ¿Se realizan copias de respaldo de la información? | **4** | | | |

| | | | | |
|---|---|---|---|---|
| 9. ¿Se lleva un seguimiento a las copias de seguridad | | **3** | | |
| 10. ¿Se cuenta con la tecnología y seguridad necesaria para evitar el sabotaje e infiltraciones? | | **4** | | |
| 11. ¿Utilizan técnicas para evitar la infección de software malicioso en los equipos de cómputo? | | **4** | | |
| 12. ¿Se realiza mantenimiento preventivo en los equipos de las dependencias? | **4** | | | |
| 13. ¿Queda un registro de ingreso y actividades de administrador en el software? | | **4** | | |
| 14. ¿Queda un registro de ingreso y actividades de usuario en el software? | | **4** | | |
| 15. ¿Posee información de los operarios que tienen acceso a cada uno de los módulos? | **4** | | | |
| 16. ¿Existe limitación de acceso a los operarios del sistema? | | **4** | | |
| 17. ¿Existen procesos para evitar que los funcionarios modificar información que no pertenece a sus funciones? | | **4** | | |
| 18. ¿Considera que el usuario y contraseña suministrados al momento de ingresar al sistema son suficientes para evitar el sabotaje o la violación a los módulos? | | **4** | | |
| **TOTAL** | **24** | **47** | | |
| **TOTAL CUESTIONARIO** | **71** | | | |

Cuadro 34. Cuestionario cuantitativo DS5. [1]

Porcentaje de Riesgo = (24*100)/(71-0) =34%
Porcentaje Riesgo total = 100-34%=66% (Riesgo Medio)

| | CUESTIONARIO CUANTITATIVO | | | REF |
|---|---|---|---|---|
| | | | | PLAN DS7 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** |
| | | | | **1 DE 1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Entregar y dar soporte (DS) | PROCESO | DS7 Educar y Entrenar a los Usuarios | |

| PREGUNTAS | SI | NO | NA | OBSERVACIÓN |
|---|---|---|---|---|
| 1. ¿Existen programas de entrenamiento en informática básica para cada grupo de empleados? | | **4** | | |
| 2. ¿Se brinda capacitación inicial a los operarios del software INFO-SALUD? | **4** | | | La capacitación inicial se brindó en el 2010 |
| 3. ¿Existen palanes para capacitación continua? | | **4** | | fecha en la q se implanto el software |
| 4. ¿Existen manuales de referencia para los usuarios de los módulos del software? | | **4** | | |
| 5. ¿Existen procedimientos para garantizar la confidencialidad, integridad y desempeño de las funciones en una forma segura? | | **4** | | |
| 6. ¿Considera que las capacitaciones brindadas contribuyen en las acciones laborales y de brindar un mejor desarrollo en sus funciones? | | **4** | | |
| **TOTAL** | **4** | **20** | | |
| **TOTAL CUESTIONARIO** | **24** | | | |

Cuadro 35. Cuestionario cuantitativo DS7. [1]

Porcentaje de Riesgo = (4*100)/(24-0) =17%
Porcentaje Riesgo total = 100-17%=83%(Riesgo Alto)

| | CUESTIONARIO CUANTITATIVO | REF | | |
|---|---|---|---|---|
| | | PLAN DS12 | | |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | **PÁGINA** | | |
| | | **1** | **DE** | **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Entregar y dar soporte (DS) | PROCESO | | DS12 Administración del Ambiente físico |

| PREGUNTAS | SI | NO | NA | OBSERVACIÓN |
|---|---|---|---|---|
| 1. ¿Existen políticas de seguridad para el control de acceso y salida de las personas que ingresa al centro de informática? | **4** | | | En la entidad se realizó una auditoria al entorno físico .y se verificó que la entidad cumple con las recomendaciones realizadas |
| 2. ¿Existen medidas físicas y ambientales que garanticen el bienestar y protección de los recursos y funcionarios? | **3** | | | |
| 3. ¿Funcionan de manera adecuada los controles en la entidad? | **3** | | | |
| 4. ¿Se cumplen con los requerimientos óptimos de seguridad en el entorno físico donde se encuentran los equipos de cómputo? | **4** | | | |
| 5. ¿En caso de una falla eléctrica, en la entidad se cuenta con una planta de energía de reserva? | **3** | | | |
| 6. ¿Se administrar de forma efectiva las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de | **3** | | | |

| | | | | |
|---|---|---|---|---|
| seguridad?<br><br>7. ¿Se encuentran identificadas las amenazas físicas por las cuales se pueden ver afectados tales como:<br><br>• Incendios<br>• robos<br>• terrorismo | **3**<br><br><br><br>**3** | **3**<br><br><br>**3**<br><br>**3** | | |
| **TOTAL** | **23** | **9** | | |
| **TOTAL CUESTIONARIO** | **32** | | | |

Cuadro 36. Cuestionario cuantitativo DS12. [1]

Porcentaje de Riesgo = (23*100)/(32-0) =72%
Porcentaje Riesgo total = 100-72%=28%(Riesgo Bajo)

| | | | | | |
|---|---|---|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | | | | **REF** PLAN DS13 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | | **PÁGINA** 1 DE 1 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | Entregar y dar soporte (DS) | PROCESO | | | DS13 Administración de Operaciones. |
| **PREGUNTAS** | | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
| 1. ¿Se realiza Mantenimiento sobre el equipo de cómputo que manejan los funcionarios?<br><br>2. ¿Existe un plan de soporte técnico en las dependencias?<br><br>3. ¿Se asigna personal especializado para realizar soporte técnico sobre los equipos | | **4**<br><br><br><br><br><br>**2** | <br><br><br>**4** | | |

| | | | | |
|---|---|---|---|---|
| de cómputo de las dependencias?<br><br>4. ¿Se tiene conciencia y se aplica sobre las medidas de prevención que se deben usar sobre los equipos, dispositivos y software para evitar complicaciones más adelante?<br><br>5. ¿El estado de la infraestructura física es apropiado y seguro para las dependencias? | **4** | **4** | | |
| **TOTAL** | **10** | **8** | | |
| **TOTAL CUESTIONARIO** | **18** | | | |

Cuadro 37. Cuestionario cuantitativo DS13. [1]

Porcentaje de Riesgo = (10*100)/(18-0) =56%
Porcentaje Riesgo total = 100-56%=44%(Riesgo Medio)

| | | | | | |
|---|---|---|---|---|---|
| | **CUESTIONARIO CUANTITATIVO** | | | **REF** | |
| | | | | PLAN DS13 | |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | **PÁGINA** | |
| | | | | **1** | **DE** **1** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | | |
| **DOMINIO** | Dominio Monitorear Y Evaluar (ME). | **PROCESO** | | ME2 Monitorear y Evaluar el Control Interno | |
| | | | | | |
| **PREGUNTAS** | | **SI** | **NO** | **NA** | **OBSERVACIÓN** |
| 1. ¿Existen procedimientos para garantizar la seguridad lógica (software) en la institución?<br><br>2. ¿Existen procedimientos para garantizar la seguridad física (servidores y equipos de cómputo)?<br><br>3. Existe una evaluación continua enfocada a mejorar el ambiente de control en cuanto | | **4** | **4** | | |

| | | | | |
|---|---|---|---|---|
| a:<br>• ¿Instalaciones?<br>• ¿Servidores?<br>• ¿Equipos de cómputo?<br>8. ¿Está definido quién es el responsable de realizar el monitoreo de evaluación?<br>9. ¿Se toman acciones correctivas de acuerdo al resultado de la evaluación del monitoreo?<br>10. ¿Existe un registro o documentación que soporte el proceso de evaluación del monitoreo realizado? | **4**<br>**4**<br>**3**<br>**4** | **4**<br>**3** | | |
| **TOTAL** | **23** | **11** | | |
| **TOTAL CUESTIONARIO** | **34** | | | |

Cuadro 38. Cuestionario cuantitativo ME2. [1]

Porcentaje de Riesgo = (23*100)/(34-0) =68%
Porcentaje Riesgo total = 100-68%=32% (Riesgo Bajo)

| | | |
|---|---|---|
| | **VALORACIÓN DE RIESGOS** | **REF** |
| | | VLRN_1 |

| **N°** | **RIESGOS/VALORACIÓN** | **PROBABILIDAD** | | | **IMPACTO** | | | **DOMINIO** |
|---|---|---|---|---|---|---|---|---|
| | | **A** | **M** | **B** | **L** | **M** | **C** | |
| R1 | No existe un diccionario de datos donde se especifique entradas y salidas (previene creación de datos incompatibles).<br><br>No existe documentación en la cual se especifique el modelo de datos, el tipo de los datos que hay en la base y la forma en que los datos se relacionan. | | **X** | | | **X** | | PO2 (1) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| R2 | No existen esquemas donde se definan niveles apropiados de seguridad y de controles de protección de datos como controles de acceso.<br><br>No existen políticas para la retención y destrucción apropiadas de información innecesaria. | | **X** | | | | **X** | PO2 (2) |
| R3 | No se encuentran definidos procedimientos para garantizar la integridad y consistencia de los datos almacenados en la base de datos. | **X** | | | | | **X** | PO2 (3) |
| R4 | No existen políticas que permitan minimizar dependencia hacia personal clave. | | **X** | | | **X** | | PO4 (1) |
| R5 | Existe rotación continua de personal. | **X** | | | | **X** | | PO7 (1) |
| R6 | No existe entrenamiento continuo para el personal con el fin de que tengan el nivel requerido para alcanzar las metas organizacionales. | **X** | | | | **X** | | PO7 (2) |
| R7 | No existen documentación de control y registro de errores presentados en el software con el fin de evitar dependencia hacia el personal clave. | | **X** | | | **X** | | PO7 (3) |
| R8 | No se toman medidas de seguridad como eliminar privilegios de acceso al Software cuándo se presenta terminación de contrato del personal. | **X** | | | | | **X** | PO7 (4) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| R9 | No existe documentación donde se identifiquen amenazas potenciales y su impacto en la prestación de servicio. | | **X** | | | | **X** | PO9 (1) |
| R10 | No existen planes eficaces de mitigación de riesgos cuando se presentan fallas en el software INFO-SALUD. | **X** | | | | | **X** | PO9 (2) |
| R11 | No existen procedimientos para especificar y acordar los requerimientos funcionales y técnicos que cubran todas las necesidades de la organización. | | **X** | | | | **X** | AI1 (1) |
| R12 | No se desarrolló un estudio de factibilidad antes de la adquisición del software | **X** | | | **X** | | | AI1 (2) |
| R13 | No existen procesos para comprobar la calidad de software de los requerimientos, políticas y procedimientos. | | **X** | | | **X** | | AI2.7 |
| R14 | No existen manuales de funcionamiento de software, que facilite la transferencia de conocimiento. | | **X** | | | | **X** | AI4 (1) |
| R15 | No existe una política formal que permita el análisis, implementación y seguimiento de cambios requeridos.<br><br>No existen procesos de revisión para garantizar la implantación completa y el correcto funcionamiento de las actualizaciones.<br><br>No se tiene documentación para usuarios finales para el manejo de cambios en algún | | **X** | | **X** | | | AI6 (1) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | módulo. | | | | | | | |
| R16 | No se estableció un entorno de pruebas donde se pueda evaluar niveles de seguridad, controles internos, calidad de datos y cargas de trabajo. | | X | | | | X | AI7 (1) |
| R17 | No existen documentos de aceptación final después de haber realizado la evaluación de requerimientos | | X | | | X | | AI7 (2) |
| R18 | La base de datos esta almacenada en Microsoft Access 2010, siendo un factor de susceptibilidad debido a los limitantes que este software tiene. | X | | | | | X | DS3(1) |
| R19 | No existen planes de contingencia efectivos donde se consideren requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los servicios. | X | | | | | X | DS4 (1) |
| R20 | No existe un plan de seguridad que garantice la protección de la información | | X | | | | X | DS5 (1) |
| R21 | Existen usuarios y contraseñas para la identificación de cada operario de INFO-SALUD, pero no se utilizan estos usuarios, se maneja una cuenta de usuario general con contraseña “1”. | X | | | | | X | DS5 (2) |
| R22 | No existen permisos de acceso de usuario al sistema, todos los operarios pueden acceder a las funciones de otros operarios. | X | | | | | X | DS5 (3) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| R23 | No se cuenta con Software antivirus que evite la infección de software malicioso | X | | | | | X | DS5 (4) |
| R24 | No existen planes que permitan identificar las necesidades de entrenamiento que deben tener empleados encargados de operar los módulos del software, ya que durante este trabajo se evidenció la necesidad de cursos de informática básica para los empleados.<br><br>No se brinda capacitación continua a los operarios del software, la última capacitación se les impartió en el año 2010.<br><br>No existen metodologías para la evaluación de planes de entrenamiento que ayuden a evaluar sus resultados y contribuir en la definición futura de los planes de entrenamiento. | X | | | | X | | DS7 (1) |
| R25 | No existe un plan de soporte técnico en las dependencias, el ingeniero encargado realiza el mantenimiento según lo crea necesario | | X | | | X | | DS(13.5) |

Cuadro 39. Valoración de riesgos. [1]

Teniendo en cuenta la probabilidad de ocurrencia y el impacto de los riesgos encontrados, se tomaron los riesgos de los módulos de la aplicación Informática INFO-SALUD que según el caso de estudio tengan mayor porcentaje de riesgo.

En el cuadro 41. Valoración de Riesgos, se enumeran los riesgos encontrados, de acuerdo al caso de estudio del trabajo, se valora los riesgos y se clasifican dentro del dominio del COBIT a los cuales corresponda según previo análisis.

**3.2.5 Pruebas realizadas.** El objetivo principal de las pruebas realizadas, fue obtener evidencia sobre los controles establecidos, su utilización, y la aplicación en los dominios de COBIT. Las evidencias son en su mayoría del personal que trabaja en la IPS Indígena Guaitara.

Junto con la presente auditoría se presentan anexos que permiten localizar las evidencias de las pruebas realizadas.

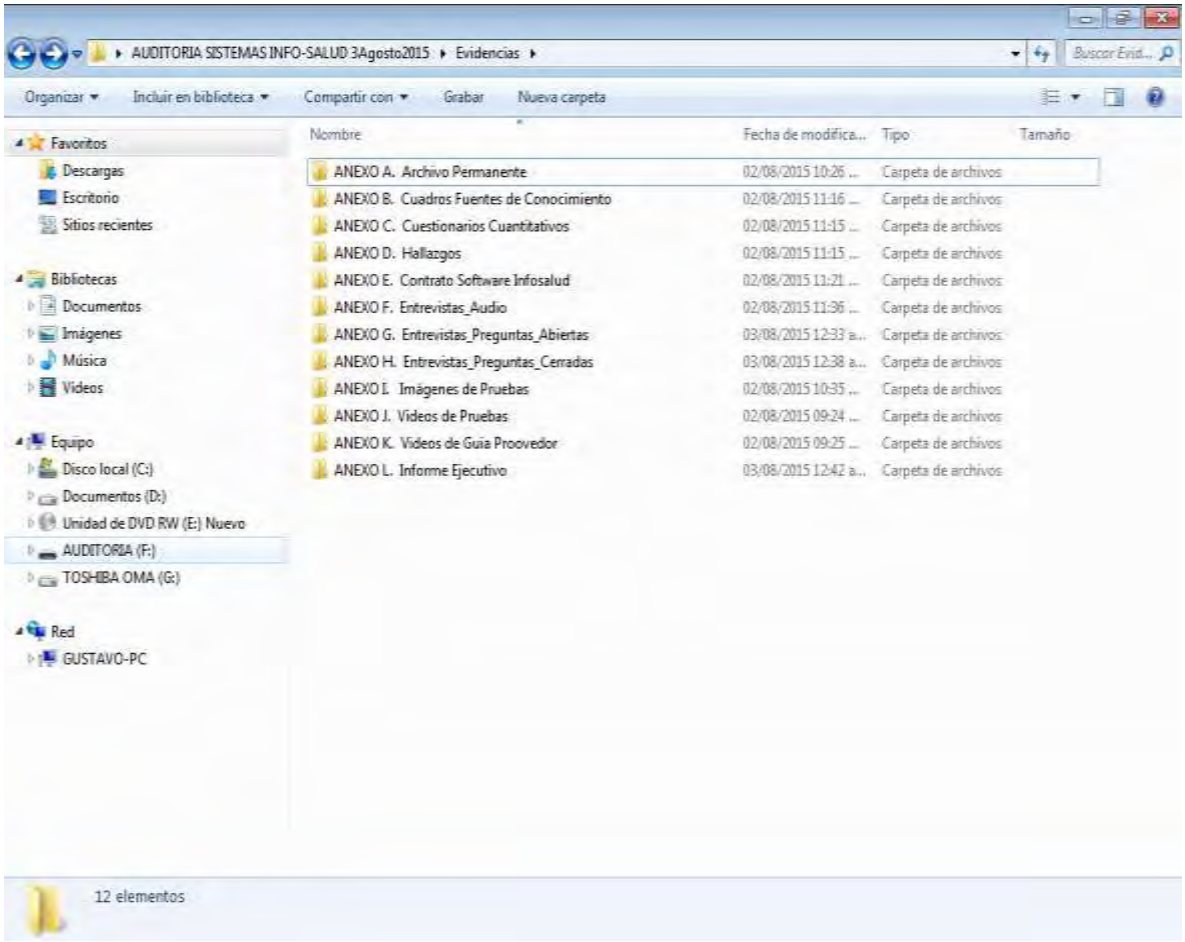



Figura 24. Organización de evidencias. [1]

A continuación, se muestra las pruebas que la auditoría presenta como soporte a los hallazgos encontrados.

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS PO2 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** . | Definir la Arquitectura de la Información |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Entrevista**  | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 | • Contiene información referente a integridad de datos. | |
| | • Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Aux_Atención_Usuario.mp3 | • Verificación de proceso de ingreso de datos en módulos correspondientes a medicina general y Facturación (Kardex | |
| | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Medico General.mp3 | | |
| | • Evidencias/ANEXO D.Entrevistas_Audio/Entrevista_IngSistemas.mp3 | • Preguntas realizadas a los empleados encargados de la operación de los módulos de INFO-SALUD | |

| | | |
|---|---|---|
| | • Evidencias/ANEXO D.Entrevistas_Audio/Entrevista2_IngSistemas.mp3 | • de datos en el software INFO-SALU |
| **Video**   | • Evidencias/ANEXO H. Videos de Guía Proveedor<br>• Evidencias/ANEXO H. Videos de Pruebas/Instalacion_tesis_INFOSALUD.mp4<br>• Evidencias/ANEXO H. Videos de Pruebas/Video_MedicinaGnrl_Clave.mp4 | |
| **Documento**   | • Evidencias/ANEXO F Entrevista_Preguntas_Cerradas<br>• Evidencias/ANEXO C. Contrato Software Infosalud | |
| **Imagen**   | • Evidencias/ANEXO G. Imágenes de pruebas | |

Cuadro 40. Pruebas realizadas PO2. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | **IPS INDÍGENA GUAITARA** | | **HDIS PO4** |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Definir los procesos, organización y relaciones de TI |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Entrevista**  | • Evidencias/ANEXO D. Entrevista Audio/Entrevista_Coordinador_Facturación.mp3<br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_Administrativo.mp3<br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_Auxiliar_Higiene_Oral.mp3<br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_IngSistemas.mp3 | • Evaluar estructuras organizacionales, roles y responsabilidades para todos los procesos permitiendo el buen funcionamiento de servicios que satisfagan los objetivos de la institución. | |

Cuadro 41. Pruebas realizadas PO4. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS PO7 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Administrar los recursos humanos de TI |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_ Administrativo.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Aux_Atención_Usuario.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Coordinacion_Facturacion.mp3<br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Personal_Kardex.mp3<br>• Evidencias/ANEXO D. | • Examinar los procesos de contratación, entrenamiento del personal y asociación de roles que correspondientes a las habilidades de los individuos. | |

| | | |
|---|---|---|
| | Entrevista_Audio/Entrevista_MedicoGeneral.mp3<br><br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_ Administrativo.mp3<br><br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_Aux_Facturacion.mp3<br><br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br><br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_Aux_Atención_Usuario.mp3<br><br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_CoordinadorDeFacturación.mp3<br><br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista2_Aux_Atención_Usuario.mp3 | |
| **VIDEOS**<br>  | • Evidencias/ANEXO H. Videos de Pruebas/Video_MedicinaGrl_Clave.mp4 | |
| **IMAGEN**<br>  | • Evidencias/ANEXO G. Imágenes de pruebas | |

Cuadro 42. Pruebas realizadas PO7. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS PO9 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | . Evaluar y Administrar los Riesgos de TI |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista_MedicoGeneral.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 | • Existencia de políticas y procedimientos para administración riesgos físicos y lógicos<br>• Evaluar existencia de planes de mitigación de riesgos cuando se presentan fallas en el software INFO-SALUD. | |

Cuadro 43. Pruebas realizadas PO9. [1]

<table>
<tr><td rowspan="2"></td><td colspan="2">PRUEBAS REALIZADAS</td><td>REF</td></tr>
<tr><td colspan="2">IPS INDÍGENA GUAITARA</td><td>HDIS AI1</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="3">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="3">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="3">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Adquirir e implementar (AI).</td><td>PROCESO</td><td>Adquirir e Implementar</td></tr>
<tr><td>PRUEBA</td><td>TIPO</td><td colspan="2">OBJETIVO</td></tr>
<tr><td>Audio<br>  </td><td>• Evidencias/ANEXO D. Entrevista Audio/MedicoAuditor.mp3<br>• Evidencias/ANEXO D. Entrevista Audio/Entrevista_AuxiliarHigieneOral.mp3</td><td colspan="2" rowspan="3">• Evaluar procedimientos para especificar y acordar los requerimientos funcionales y técnicos.</td></tr>
<tr><td>IMAGEN<br>  </td><td>• Evidencias/ANEXO G. Imágenes de pruebas</td></tr>
<tr><td>DOCUMENTOS<br>  </td><td>• Evidencias/Documentos_AdquisicionSoftware</td></tr>
</table>

Cuadro 44. Pruebas realizadas PO9. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS AI4 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Facilitar la Operación y el Uso |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/Entrevista_Audio/Entrevista2_PersonalEncargadoDeKardex.mp3<br>• Evidencias/Entrevista_Audio/ Entrevista_PersonalEncargadoDeKardex.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3 | • Evaluar la existencia de procesos para comprobar la calidad de software<br>• Evaluar el cumplimiento de los requerimientos, políticas y procedimientos solicitados por la entidad. | |
| **IMAGEN**   | • Evidencias/ANEXO G. Imágenes de pruebas | | |

Cuadro 45. Pruebas realizadas PO9. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS AI6 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | Administrar cambios |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3 | • Evaluar existencia de políticas formales que permita el análisis, implementación y seguimiento de cambios requeridos. | |
| | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3 | • Existencia de procesos de revisión para garantizar el correcto funcionamiento de las actualizaciones | |
| | • Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara | • Documentación para usuarios finales para el manejo de cambios en algún módulo. | |

Cuadro 46. Pruebas realizadas AI6. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS AI7 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e implementar (AI). | **PROCESO** | Instalar y Acreditar Soluciones y Cambios |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO F. Entrevistas_Preguntas _Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entr evista_MedicoGeneral .mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entr evista_MedicoAuditorl. mp3.<br>• Evidencias/Entrevista_ Audio/Entrevista2_Ing Sistemas.mp3<br>• Evidencias/Entrevistas _Audio/Entrevista_Dir ectorAdministrativo.mp 3 | • Evaluar la existencia de plan de implantación para el aplicativo informático INFO-SALUD el cual debe tener bien definido actividades como recursos necesarios de software y hardware mínimos necesarios para la instalación del aplicativo, pruebas para comprobar que el sistema esté totalmente operativo,<br>• Entrevista Ingeniero encargado del centro de informática de la IPS con el fin de evaluar si el proceso de implementación anteriormente descrito se realizó satisfactoriamente.<br>• Entrevistas personal encargado del aplicativo informático con el fin de evaluar proceso de capacitación y asistencia. | |
| **DOCUMENTOS**   | • Evidencias/Document os_AdquisicionSoftwar e | | |

Cuadro 47. Pruebas realizadas AI7. [1]

<table>
<tr><td rowspan="2"></td><td colspan="3">PRUEBAS REALIZADAS</td><td>REF</td></tr>
<tr><td colspan="3">IPS INDÍGENA GUAITARA</td><td>HDIS DS3</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="4">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="4">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="4">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Entregar y dar soporte (DS).</td><td>PROCESO</td><td>Administrar el desempeño y la capacidad</td></tr>
<tr><td>PRUEBA</td><td colspan="2">TIPO</td><td colspan="2">OBJETIVO</td></tr>
<tr><td>Audio<br>  <br></td><td colspan="2">• Evidencias/ANEXO F. Entrevistas_Preguntas_ Cerradas/entrevista ingeniero (1)<br>• Evidencias/ANEXO F. Entrevistas_Preguntas_ Cerradas/entrevista ingeniero (2)<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3</td><td colspan="2" rowspan="3">• Evaluar estabilidad, Respaldo de Archivos, Escalabilidad, Seguridad o Capacidad de Almacenamiento.<br>• Analizar el plan de seguimiento evaluativo a las fallas que presenta el software</td></tr>
<tr><td>VIDEOS<br>  <br></td><td colspan="2">• Evidencias/ANEXO H. Videos de Pruebas/demostracion_ accespv.mp4</td></tr>
<tr><td>IMAGEN<br>  <br></td><td colspan="2">• Evidencias/ANEXO G. Imágenes de pruebas</td></tr>
</table>

Cuadro 48. Pruebas realizadas DS3. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS DS4 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | Garantizar la Continuidad del Servicio |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditor.mp3<br>• Evidencias/ANEXO D. Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Atención_Usuario.mp3<br>• Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Coordinacion_Facturacion.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Facturación.mp3 | • Existencia de planes de contingencia<br>• Sesiones de entrenamiento para procedimiento a realizarse en caso de interrupciones no planeadas. | |

Cuadro 49. Pruebas realizadas DS4. [1]

| | PRUEBAS REALIZADAS<br>IPS INDÍGENA GUAITARA | | REF<br>HDIS DS5 |
|---|---|---|---|
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLE** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS). | **PROCESO** | Garantizar la Seguridad de los Sistemas |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**  | • Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Atención_Usuario.mp3 | • Existencia de usuarios y contraseñas para la identificación de cada operario de INFO-SALUD<br>• Evaluar permisos de acceso de usuario al sistema | |
| **IMAGEN**  | • Evidencias/Evidencias/ANEXO G. Imágenes de pruebas | • Análisis de medidas preventivas, detectivas y correctivas en la institución para proteger los sistemas de la información | |
| **DOCUMENTOS**  | • Evidencias/ANEXO E. Entrevistas_Preguntas_Abiertas<br>• Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara | | |

Cuadro 50. Pruebas realizadas DS5. [1]

<table>
<tr><td rowspan="2"></td><td colspan="3">PRUEBAS REALIZADAS</td><td>REF</td></tr>
<tr><td colspan="3">IPS INDÍGENA GUAITARA</td><td>HDIS DS7</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="4">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="4">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="4">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Entregar y dar soporte (DS).</td><td>PROCESO</td><td colspan="2">Educar y Entrenar a los Usuarios</td></tr>
<tr><td>PRUEBA</td><td colspan="2">TIPO</td><td colspan="2">OBJETIVO</td></tr>
<tr><td>Audio<br>  </td><td colspan="2">• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>• Evidencias /Entrevista Audio/Entrevista_Aux_Facturación</td><td colspan="2" rowspan="3">• Evaluar la existencia de capacitación continua a los operarios del software</td></tr>
<tr><td>VIDEOS<br>  </td><td colspan="2">• Evidencias/Videos_Desarrollador Evidencias/Instalacion_tesis_INFOSALUD.mp4</td></tr>
<tr><td>DOCUMENTOS<br>  </td><td colspan="2">• Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara</td></tr>
</table>

Cuadro 51. Pruebas realizadas DS7. [1]

<table>
<tr><td rowspan="2"></td><td colspan="2">PRUEBAS REALIZADAS</td><td>REF</td></tr>
<tr><td colspan="2">IPS INDÍGENA GUAITARA</td><td>HDIS DS12</td></tr>
<tr><td>OBJETO DE ESTUDIO</td><td colspan="3">Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD</td></tr>
<tr><td>RESPONSABLES</td><td colspan="3">Mauricio Aza Arévalo – Mélanny Oviedo Mesías</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="3">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Entregar y dar soporte (DS).</td><td>PROCESO</td><td>Administración de Ambiente Físico.</td></tr>
<tr><td>PRUEBA</td><td>TIPO</td><td colspan="2">OBJETIVO</td></tr>
<tr><td>Audio<br>  </td><td>• Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3<br>• Evidencias /Entrevista Audio/Entrevista_CoordinadorDeFacturación.mp3</td><td colspan="2" rowspan="4">• Evaluar la protección de los activos de cómputo y la información de la entidad</td></tr>
<tr><td>VIDEOS<br>  </td><td>• Evidencias\ANEXO J. Videos de Pruebas/ Demostracion_accespv<br>• Evidencias\ANEXO J. Videos de Pruebas/ Video_MedicinaGrl_Clave</td></tr>
<tr><td>IMAGEN<br>  </td><td>• Evidencias\ANEXO G. Imágenes de Pruebas</td></tr>
<tr><td>DOCUMENTOS<br>  </td><td>• Evidencias\ANEXO F. Entrevistas_Preguntas_ Cerradas<br>• Evidencias\ANEXO E. Entrevistas_Preguntas_ Abiertas</td></tr>
</table>

Cuadro 52. Pruebas realizadas DS12. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS DS13 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y dar soporte (DS) | **PROCESO** | Administración de Operaciones. |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias/ANEXO D. Entrevista Audio/Entrevista_CoordinadorDeFacturación.mp3<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 | • Analizar la efectividad en la administración y protección de datos de salida sensitivos | |
| **VIDEOS**   | • Evidencias\ANEXO J. Videos de Pruebas/ Demostracion_accespv<br>• Evidencias\ANEXO J. Videos de Pruebas/ Video_MedicinaGrl_Clave | | |
| **IMAGEN**   | • Evidencias\ANEXO G. Imágenes de Pruebas | | |
| **DOCUMENTOS**   | • Evidencias\ANEXO E. Entrevistas_Preguntas_Abiertas | | |

Cuadro 53. Pruebas realizadas DS13. [1]

| | PRUEBAS REALIZADAS | | REF |
|---|---|---|---|
| | IPS INDÍGENA GUAITARA | | HDIS ME2 |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Monitorear Y Evaluar (ME). | **PROCESO** | Excepciones de Control |
| **PRUEBA** | **TIPO** | **OBJETIVO** | |
| **Audio**   | • Evidencias\ANEXO D. Entrevistas_Audio/ Entrevista2_IngSistemas<br>• Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 | • Analizar la existencia de procesos de monitoreo TI | |
| **DOCUMENTOS**   | • Evidencias\ANEXO F. Entrevistas_Preguntas_ Cerradas/ entrevista ingeniero (1)<br>• Evidencias\ANEXO F. Entrevistas_Preguntas_ Cerradas/ entrevista ingeniero (2) | | |

Cuadro 54. Pruebas realizadas ME2. [1]

Para observar la totalidad de pruebas realizadas en el proceso de auditoría al software INFO-SALUD, ver la carpeta **EVIDENCIAS** que se encuentra de manera digital en el DVD que se anexa en el trabajo.

### 3.2.6 Hallazgos de módulos pertenecientes al software INFO-SALUD

A continuación, se describen las posibles amenazas encontradas en el funcionamiento, adquisición, implementación y uso de los módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD.
Dominios y Procedimientos Auditados en los módulos pertenecientes al Software INFO-SALUD

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN (PO).

PO2: Definir la arquitectura de la información.
PO4: Definir los procesos, organización y relaciones de TI.
PO7: Administrar los recursos humanos de TI
PO9: Evaluar y administrar los riesgos de TI

DOMINIO: ADQUIRIR E IMPLEMENTAR (AI).

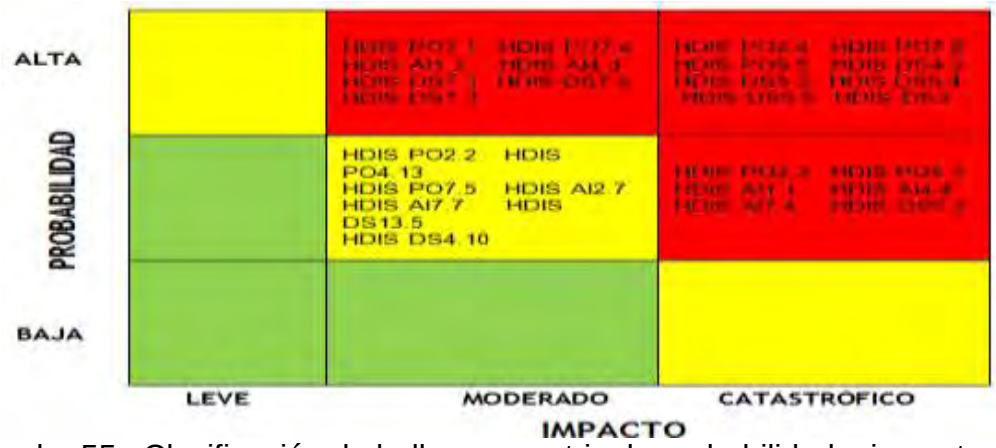
AI1: Identificar soluciones automatizadas
AI2: Adquirir y mantener software aplicativo
AI4: Facilitar la operación y el uso
AI6: Administrar cambios
AI7: Instalar y acreditar soluciones y cambios

DOMINIO: ENTREGAR Y DAR SOPORTE (DS).

DS3: Instalar y acreditar soluciones y cambios
DS4: Garantizar la continuidad del servicio
DS5: Garantizar la seguridad de los sistemas
DS7: Educar y entrenar a los usuarios
DS12: Administración del ambiente físico
DS13: Administración de operaciones

DOMINIO: MONITOREAR Y EVALUAR (ME).

ME2: Monitorear y evaluar el control interno




Cuadro 55. Clasificación de hallazgos matriz de probabilidad e impacto. [1]

A continuación, se detallan los hallazgos encontrados organizados por dominios, explicando sus consecuencias y las recomendaciones que el grupo auditor consideró pertinentes.

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** HDIS PO2 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Definir la Arquitectura de la Información. |
| **HALLAZGO** | | | |
| No existe un diccionario de datos donde se recolecta, confirme y se especifique entradas y salidas de datos.<br><br>No existe un diccionario de datos donde se describa la clasificación de usuarios, niveles de acceso y restricciones.<br><br>No existen diagramas de flujo de los módulos de datos o pseudocódigo de las partes de los módulos y sus especificaciones del software INFO-SALUD.<br><br>No existen esquemas de diseño donde se detallen la lógica de los procesos que se administran desde el software INFO-SALUD. | | | |
| **CONSECUENCIAS** | | | |
| La falta de un diccionario de datos, genera desinformación de los detalles y descripción de los datos almacenados en el sistema informático (nombre, descripción, alias, contenido).<br><br>La inexistencia de documentación de respaldo, acerca de los detalles del sistema informático como procesos realizados, donde se emplean los datos y los sitios donde se necesita el acceso inmediato a la información, puede dar malas interpretaciones o ambigüedades por parte de los ingenieros encargados de administrar los procesos del software.<br><br>La falta de diagramas y diseños que permitan entender los procesos que soporta el software INFO-SALUD dificulta eventuales correcciones, mantenimientos y ampliaciones que requiera la herramienta informática. | | | |
| **RECOMENDACIONES** | | | |

| |
|---|
| Documentar el diccionario de datos de los módulos del software INFO-SALUD e Incorporar dentro del diccionario de datos descripción detallada de:<br><br>• Entradas y salidas de datos.<br>• Clasificación de tipos de usuarios<br>• Niveles de acceso y las restricciones para el ingreso<br><br>Tener actualizado el diccionario de datos ante cambios o implementación de nuevas funcionalidades. |
| **PROBABILIDAD E IMPACTO** |
| Probabilidad: Media<br>Impacto: Medio |

| | |
|---|---|
| **EVIDENCIAS** | Evidencias/Entrevista_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/Entrevista_Audio/Entrevista_Aux_Atención_Usuario.mp3<br>Evidencias/ANEXO C. Contrato Software Infosalud<br>Evidencias/ANEXO I. Videos de Guia Proovedor |

Cuadro 56. Hallazgos PO2. [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS PO2 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Definir la Arquitectura de la Información. |
| **HALLAZGO** | | | |
| No existen esquemas de clasificación de la información basada en que tan confidencial son los datos administrados por la aplicación.<br><br>No existen esquemas documentados donde se definan niveles apropiados de seguridad y de controles de protección de datos como controles de acceso que eviten que información privilegiada sea vista por todos los usuarios con acceso al software INFO-SALUD. | | | |

| |
|---|
| No existe un plan de seguridad en los procesos que se manejan en el software INFO-SALUD, que garantice la integridad y consistencia de los datos almacenados en formato electrónico. |
| **CONSECUENCIAS** |
| La falta de esquemas documentados de clasificación de la información no permite identificar qué información es relevante y de carácter privado para la empresa incurriendo en riesgos de perdida de información.<br><br>La información representa uno de los activos más importantes de la empresa, por ello los procesos que no se hagan siguiendo un plan de seguridad ponen en riesgo la conservación, integridad y consistencia de los datos almacenados. |
| **RECOMENDACIONES** |
| Establecer controles de acceso a los módulos del aplicativo informático INFO-SALUD como contraseñas personales que permiten seguridad de información privilegiada del paciente y la visualización solo del personal médico evitando que personal de otras secciones como inventarios o citas, que tiene acceso al software INFO-SALUD puedan ver información de carácter privado.<br><br>Para la correcta administración y salvaguarda de la información se hace necesario implantar un plan de seguridad en los procesos que son soportados por la aplicación informática INFO-SALUD tales como:<br><br>• Ingreso de datos y verificación de validación en cumplimiento de normas establecidas en el software.<br><br>• Almacenamiento periódico de información en copias de seguridad administradas por el área especializada (auditoría, sistemas, etc).<br><br>• Garantizar que la información sea accesible y utilizable solo por el personal autorizado. |
| **PROBABILIDAD E IMPACTO** |
| Probabilidad: Media<br>Impacto: Catastrófico |

| | |
|---|---|
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO H. Videos de Pruebas/Video_MedicinaGnrl_Clave.mp4 |

Cuadro 57. Hallazgos PO2(2). [1]

| . | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS PO2 (3) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Definir la Arquitectura de la Información. |

**HALLAZGO**

No existe un manual de diseño del software donde se especifiquen requerimientos del software y hardware para su funcionamiento.

No existe documentación donde se describa la configuración y funcionamiento del software.

No existen diagramas de flujo de datos o pseudocódigo de las partes de los módulos y sus especificaciones.

**CONSECUENCIAS**

La falta de documentación que describa el diseño y funcionamiento del software genera riesgo de pérdida de completitud, exactitud o precisión del activo informático. Ejemplo: Errores de procesamiento de los sistemas informáticos debido a no cumplir los requerimientos mínimos de hardware.

El desconocimiento de configuración y funcionamiento debido a la inexistencia de documentación que sirva de referencia, genera dependencia hacia el proveedor del software debido a que solo él, conoce aspectos de configuración y funcionamiento que son necesarios para eventuales correcciones o mantenimientos.

Los diagramas de flujo de datos son representaciones graficas que facilitan el comprender como funciona el software a nivel de entradas, procesos y salidas de información, cuando no se poseen estos diagramas no se puede comprender fácilmente como funciona un módulo en el software INFO-SALUD por parte del personal del área de sistemas de la IPSI GUAITARA.

**RECOMENDACIONES**

En futuras negociaciones solicitar al ingeniero proveedor del software documentación en donde se incluya documentación de soporte como:

- Manual de diseño de software

<table>
<tr><td colspan="2">
<ul>
<li>Requerimientos de software</li>
<li>Requerimientos de hardware</li>
</ul>
Con el objetivo de que la entidad, logre cumplir con las condiciones necesarias para que la aplicación informática INFO-SALUD, funcione correctamente.<br><br>
En el contrato de renovación del software INFO-SALUD o adquisición de otro software, la IPSI GUAITARA debe incluir cláusulas en donde se especifiquen:
<ul>
<li>Requerimientos Funcionales de la IPSI GUAITARA</li>
<li>Condiciones técnicas y especificas del software</li>
<li>Documentación de soporte</li>
<li>Etapas y tiempos en la implementación del software en las fases de:
<ul>
<li>Planeación</li>
<li>Diseño</li>
<li>Configuración</li>
<li>Pruebas</li>
<li>Capacitación</li>
<li>Preparación</li>
<li>Estabilización</li>
</ul>
</li>
</ul>
Requerir que el software garantice la integridad de los datos mediante la implementación de:
<ul>
<li>Reglas de normalización de datos</li>
<li>Integridad referencial</li>
<li>Validación de los datos</li>
</ul>
</td></tr>
<tr><td colspan="2">PROBABILIDAD E IMPACTO</td></tr>
<tr><td colspan="2">Probabilidad: Alta<br>Impacto: Catastrófica</td></tr>
<tr><td>EVIDENCIAS</td><td>Evidencias/ANEXO D.Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO D.Entrevistas_Audio/Entrevista2_IngSistemas.mp3</td></tr>
</table>

Cuadro 58. Hallazgos PO2(3). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS PO 4 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Definir los Procesos, Organización y Relaciones de TI. |

**HALLAZGO**

Existe dependencia excesiva hacia el personal que posee experiencia en el manejo del software INFO-SALUD, ya que no existen políticas que permitan replicar el conocimiento sobre el manejo del aplicativo por parte de estos empleados.

**CONSECUENCIAS**

La dependencia en personal clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone al sistema informático en manos de pocas personas, siendo esto un riesgo, ya que si estas personas salen de la institución, esta podría verse afectada en el funcionamiento de sus procesos.

Este personal especializado, con frecuencia posee la experiencia y el conocimiento único y no registrado de las modificaciones o el funcionamiento del software. La supervisión y el control de su trabajo resulta difícil debido a la dependencia excesiva hacia este personal.

**RECOMENDACIONES**

Identificar al personal clave de recursos TI y minimizar la dependencia de la institución hacia este personal, por ello es necesario tener planes estratégicos y tácticos para la captura documental del conocimiento, con el fin de organizar los documentos requeridos en donde se especifique una bitácora de los errores más frecuentes presentados en el software y las soluciones a implementarse.

Implementar planes de entrenamiento para el personal nuevo, con el fin de lograr la calidad deseada por la entidad.

La entidad debe tener los manuales de funcionamiento de software actualizados y al alcance de los empleados asignados a TI, esto permite el apoyo para el buen ejercicio de sus actividades.

| PROBABILIDAD E IMPACTO | |
|---|---|
| Probabilidad: Media<br>Impacto: Leve | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevista Audio/Entrevista_Coordinador_Facturación.mp3<br>Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_ Administrativo.mp3<br>Evidencias/ANEXO D. Entrevista Audio/ Entrevista_Auxiliar_Higiene_Oral.mp3 |

Cuadro 59. Hallazgos PO4. [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS PO7 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Administrar los Recursos Humanos de TI. |
| **HALLAZGO** | | | |
| Se observó rotación y desvinculación continúa de personal asignado a TI por razones ajenas a la institución. | | | |
| **CONSECUENCIAS** | | | |
| La Rotación de personal trae consigo gastos como:<br>• Costo de Reclutamiento y Selección<br>• Costo de Admisión<br>• Costo de Registro y Documentación<br>• Costo de Ingreso<br>• Costo de Desvinculación<br>• Costos de Capacitación | | | |

| | |
|---|---|
| Los cuales son perjudiciales financieramente para la organización, debido a que la vinculación y desvinculación del personal promueve la contratación de nuevos empleados para que desempeñen las actividades de los puestos vacantes. | |
| **RECOMENDACIONES** | |
| Los motivos del continuo cambio de personal equivalen a razones gubernamentales, es necesario implementar políticas gerenciales que permitan analizar las posibles amenazas que acarrea la rotación de personal y mitigar sus efectos negativos en la Institución.<br><br>Generar una política de entrenamiento que este soportada por una serie de manuales de procedimientos, los cuales deben tener guías prácticas donde se describan con detalle las funciones a realizar, funcionamiento del módulo del software que va administrar y una bitácora de errores con sus respectivas soluciones, logrando así que el conocimiento adquirido por las personas que terminan su contrato quede registrado para ser utilizado por los nuevos empleados, permitiendo minimizar gastos de entrenamiento y tener un buen nivel de rendimiento y productividad del nuevo personal. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta<br>Impacto: Moderado | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_ Administrativo.mp3<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Aux_Atención_Usuario.mp3 |

Cuadro 60. Hallazgos PO7(1)

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS PO 7 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Administrar los Recursos Humanos de TI. |

**HALLAZGO**

No existe entrenamiento continuo orientado al personal.

El ingeniero proveedor del software realizó una capacitación inicial en el año 2010, fecha en la cual se adquirió el software, posterior a este facha no se han realizado capacitaciones pese a las actualizaciones y cambios funcionales en los módulos del software.

Dificultad de los empleados nuevos asignados al manejo del aplicativo INFO-SALUD para llevar a cabo su trabajo, ya que no se realizó la capacitación necesaria, además no existe un manual de software que les permita conocer su manejo.

**CONSECUENCIAS**

El entrenamiento mantiene a los empleados enfocados y al día sobre las maneras más efectivas de hacer su trabajo, sin entrenamiento, los empleados tienen menos probabilidades de completar las tareas de forma efectiva y con eficacia suficiente.

Puede causar traumas de tiempo en la prestación de los servicios de la Institución reduciendo drásticamente la buena imagen de esta.

Una vez que la calidad en el servicio se reduce, se vuelve más difícil dedicar tiempo y dinero a la capacitación y al mantenimiento del software.

A los empleados les toma más tiempo familiarizarse con el sistema con el que laboran debido a la no existencia de un manual de software.

**RECOMENDACIONES**

Establecer procesos de capacitación dirigidos a los operarios de los módulos del software que debe incluir:

| |
|---|
| • Charlas acerca del funcionamiento del software.<br>• Manuales de usuario donde se especifique su funcionalidad.<br><br>La capacitación debe ser obligatoria y continua, ya que es un factor importante que ayuda a los empleados a ser competitivos y más eficientes, dando como resultado una excelente prestación de servicio a los usuarios. |
| **PROBABILIDAD E IMPACTO** |
| Probabilidad: Alta<br>Impacto: Moderado |

| | |
|---|---|
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Coordinacion_Facturacion.mp3<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Personal_Kardex.mp3<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista_MedicoGeneral.mp3 |

Cuadro 61. Hallazgos PO7(2). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS PO7 (3) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Administrar los Recursos Humanos de TI. |
| **HALLAZGO** | | | |
| No existen documentación de control y registro de errores presentados en el software INFO-SALUD con el fin de evitar dependencia del personal calificado. | | | |
| **CONSECUENCIAS** | | | |

| | |
|---|---|
| En la entidad no existe documentación técnica sobre el manejo del software, registro de funcionalidades o medidas en caso de errores, este tipo de información solo se transfiere de persona a persona, lo cual conlleva a que se dé información errónea o que se realice procesos mal ejecutados por desconocimiento además se puede generar dependencia del personal con experticia en el funcionamiento de los módulos.<br><br>La dependencia de trabajadores expertos en el manejo del aplicativo informático, puede causar retrasos en los procesos que dependen y soporta la herramienta informática, cuando estos empleados dejan de trabajar para la institución, puesto que los tiempos de adaptación del nuevo personal toman su tiempo en adaptación y capacitación. | |
| **RECOMENDACIONES** | |
| Implementar procesos de documentación de gestión del conocimiento que promuevan la captura, evaluación, recuperación, preservación y aprovechamiento del conocimiento y la experticia de los empleados encargados de la operación de los módulos del software INFO-SALUD en la institución, con el fin de generar una retroalimentación positiva en los procesos soportados por este software para evitar la dependencia de este personal calificado en la organización y tener un archivo de documentos sobre el manejo del software y sus funcionalidades.. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Medio<br>Impacto: Moderado | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevista Audio/Entrevista_Director_ Administrativo.mp3<br>Evidencias/ANEXO D. Entrevista Audio/Entrevista_Aux_Facturacion.mp3<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO D. Entrevista Audio/Entrevista_Aux_Atención_Usuario.mp3<br>Evidencias/ANEXO D. Entrevista Audio/Entrevista_CoordinadorDeFacturación.mp3 |

Cuadro 62. Hallazgos PO7(3). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS PO7 (4) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Administrar los Recursos Humanos de TI. |

**HALLAZGO**

No se toman medidas de seguridad como eliminar privilegios de acceso al Software cuándo se presenta terminación de contrato del personal calificado en el manejo del aplicativo INFO-SALUD.

**CONSECUENCIAS**

La falta de control en la administración de los privilegios de acceso para el ingreso al aplicativo INFO-SALUD, genera fallas en la seguridad de la información, ya que el personal que ha terminado el contrato con la institución aún tienen activos sus privilegios para ingresar a información confidencial que podrían modificar, esto puede causar inconsistencias, falta de veracidad de la información y riesgos de alteración.

**RECOMENDACIONES**

Establecer políticas generales para la gestión de seguridad informática que establezcan estrategias como:

- Administración de cuentas de usuarios.
- Administración de contraseñas de usuarios.
- Verificación de usos por parte los de usuario, contraseñas y niveles de seguridad.
- Concientización de los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y sistemas computacionales.

Mantener un archivo de auditoría o logs, donde sean registradas todas las operaciones realizadas por los usuarios; en caso de sospecha de falla en la seguridad de este sistema informático, los archivos de log podrán ser consultados para conocer el autor y los daños causados por operaciones

| | |
|---|---|
| irregulares.<br><br>Instituir estrategias para evaluar el cumplimiento de las pautas establecidas y relacionadas con control de acceso, creación de usuarios, administración de privilegios, autenticación de usuarios y uso controlado de utilitarios del software.<br><br>Una buena administración de la seguridad puede permitir mayor control de las actividades de los usuarios sobre el sistema informático. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/ANEXO H. Videos de Pruebas/Video_MedicinaGrl_Clave.mp4<br>Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista2_Aux_Atención_Usuario.mp3 |

Cuadro 63. Hallazgos PO7(4). [1]

| | | | | |
|---|---|---|---|---|
| | **HALLAZGOS** | | | **REF** |
| | | | | HDIS PO9 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | | |
| **MATERIAL DE SOPORTE** | COBIT | | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Evaluar y Administrar los riesgos TI | |
| **HALLAZGO** | | | | |
| No existen políticas y procedimientos para administración de riesgos físicos y lógicos alrededor del aplicativo informático INFO-SALUD. | | | | |
| **CONSECUENCIAS** | | | | |
| La falta de procesos para la administración de riegos TI impide la detección de riesgos y vulnerabilidades, las cuales generan riesgos informáticos que incluyen pérdida de productividad debido al tiempo de inactividad del software, brechas de seguridad que exponen la información de los usuarios de la IPS, multas por violaciones de normas y la imposibilidad de soportar demandas debido a la custodia inadecuada de registros e información. | | | | |

| **RECOMENDACIONES** | |
|---|---|
| Implementar una política de administración efectiva de vulnerabilidades en la institución, con el fin de hacer frente a los riesgos informáticos; esta política debe ayudar a priorizar y planificar:<br><br>• Opciones de mitigación de riesgos informáticos.<br><br>• Calcular los impactos en la prestación de servicios a causa de los riesgos informáticos.<br><br>• Diseñar soluciones orientadas a mitigar los riesgos informáticos.<br><br>• Priorizar los riesgos informáticos.<br><br>• Evaluar los costos para optimizar las inversiones.<br><br>• Administrar y mitigar los riesgos informáticos de manera continua.<br><br>La política de administración de riesgos debe incluir estrategias que permita:<br><br>• Priorizar y establecer niveles de riesgo para los procesos y recursos empresariales críticos.<br><br>• Pasar de un enfoque de mitigación del riesgo a prevenir proactivamente las fallas.<br><br>• Tomar decisiones orientadas a la manera de proteger los activos de la institución.<br><br>• Evaluar las tácticas, técnicas y los costos de administración de riesgos relacionados con los diferentes niveles de protección informática. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media<br>Impacto: Medio. | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO D. Entrevista_Audio/Entrevista_MedicoGeneral.mp3 |

Cuadro 64. Hallazgos PO9(1). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS PO9 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Planeación y Organización | **PROCESO** | Evaluar y Administrar los riesgos TI |

**HALLAZGO**

No existen planes eficaces de mitigación de riesgos cuando se presentan fallas en el software INFO-SALUD.

**CONSECUENCIAS**

Cualquier entidad está expuesta al riesgo de interrupción del servicio por diversas causas, siendo las más frecuentes las relacionadas con fallas en los sistemas informáticos, siendo uno de los ejes de la operatividad de una organización, puede ser vulnerable debido a riesgos informáticos y por lo tanto, se debe estar preparados para cualquier eventualidad. Por lo tanto, es pertinente crear y fortalecer una conciencia colectiva sobre la trascendencia del tema de recuperación en caso de desastres.

**RECOMENDACIONES**

Definir, implementar, probar y mantener un proceso para administrar la continuidad del servicio informático, que incluya elementos como:

- Prevención y atención de emergencias
- Administración de la crisis
- Plan de contingencias
- Capacidad de retorno a la operación normal

El plan de contingencia orientado al sistema informático deben cumplir, como mínimo con los siguientes requisitos:

- Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.
- Ser conocidos por todos los involucrados

| | |
|---|---|
| • Cubrir por lo menos los siguientes aspectos: identificación de eventos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y retorno a las actividades normales<br><br>• Efectuar periódicamente de manera cronológica un diagnóstico sobre la situación de los sistemas informáticos que incluya análisis de riesgos y su variación en los niveles<br><br>• Observar los protocolos y procedimientos establecidos para la protección de la información y garantizar la preservación de la memoria institucional | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Catastrófica. | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 |

Cuadro 65. Hallazgos PO9(2). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS AI1 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Identificar Soluciones Automatizadas |
| **HALLAZGO** | | | |
| No existen procedimientos para especificar y acordar los requerimientos funcionales y técnicos que cubran todas las necesidades informáticas de la organización. | | | |
| **CONSECUENCIAS** | | | |

La IPSI Guaitara es una institución prestadora de servicio de salud de nivel I y el software encargado de la administración de los principales procesos que se llevan a cabo en esta entidad está desarrollado para una entidad de nivel II, por lo cual existen procedimientos implementados en el software para unidades que no existen en la IPS como urgencias y hospitalización; además debido a la falta de la implementación de un proceso para la gestión de requerimientos necesarios para la atención de calidad a los beneficiarios, se evidenció:

- Falta de formatos de evaluación nutricional para madres gestantes.

- Graficas de control de crecimiento y desarrollo.

**RECOMENDACIONES**

Implementar un proceso de adquisición de software para la gestión de requerimientos y requisitos, donde exista una especificación de requerimientos funcionales y no funcionales completa y consistente con el fin de cubrir todas las necesidades de la institución en cuanto a los procesos manejados en la misma.

En el proceso de generación de requerimientos que complementen al sistema informático, se deben tener en cuenta:

- Requerimientos del producto, donde se especifiquen el comportamiento del software.

- Requerimientos de desempeño, donde se describan la eficiencia de ejecución del sistema informático y requerimientos de hardware.

- Requerimientos de fiabilidad, que fijen la tasa de fallas para que el sistema sea aceptable.

- Requerimientos de usabilidad, describen los niveles apropiados de usabilidad dados los usuarios finales del producto, para ello deben revisarse las especificaciones de los usuarios como rendimiento de la aplicación, facilidad de aprendizaje, velocidad de operación, entre otros.

- Requerimientos organizacionales, se derivan de las políticas y procedimientos existentes en la organización orientados al sistema informático.

- Requerimientos de entrega, que especifiquen cuándo se entregará el producto informático y su documentación.

- Requerimientos externos, se derivan de los factores externos al sistema informático y de su proceso de desarrollo.

| | |
|---|---|
| • Requerimientos de Interoperabilidad, que definen la manera en que el sistema informático interactúa con los otros sistemas de la organización<br><br>• Requerimientos Legales, que deben seguirse para asegurar que el sistema informático opere dentro de las normas y leyes. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media.<br>Impacto: Catastrófica. | |
| **EVIDENCIAS** | Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO D. Entrevista Audio/MedicoAuditor.mp3<br>Evidencias/ANEXO D. Entrevista Audio/Entrevista_AuxiliarHigieneOral.mp3 |

Cuadro 66. Hallazgos AI1(1). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS AI1 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas AA Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Identificar Soluciones Automatizadas |
| **HALLAZGO** | | | |
| No se realizó un estudio de factibilidad antes de la adquisición del software | | | |
| **CONSECUENCIAS** | | | |
| La falta de planificación para la adquisición de software puede generar inconsistencias debido a la imprecisión de los requerimientos necesarios para la organización y puede desmejorar el servicio que se presta a los beneficiarios de la entidad, así como también puede alterar los procesos que debe soportar el software o aplicativo informático. | | | |
| **RECOMENDACIONES** | | | |
| Definir políticas formales de factibilidad para la adquisición de software en el cual se deben establecer las razones que amerita la adquisición de un nuevo sistema informático, capacidad técnica que implique la implantación del sistema en cuestión, así como estudio y análisis de costos, beneficios y el grado de | | | |

| |
|---|
| aceptación que la propuesta genera en la Institución; los aspectos tomados en cuenta deben ser:<br><br>• Factibilidad Técnica la cual consiste en la evaluación de la tecnología existente en la organización.<br><br>• Factibilidad Económica donde se analizarán los recursos necesarios para implantar y mantener en operación del sistema.<br><br>• Análisis Costos-Beneficios: Este análisis permite hacer una comparación entre la relación del sistema actual y los costos que tendrá la implementación de un nuevo software.<br><br>• Costo de personal: en donde se incluyen los beneficios en horas de producción que presentan los operadores con la nueva adquisición.<br><br>• Estudio de factibilidad lógica.<br><br>• Estudio y análisis de requerimientos del sistema informático |
| **PROBABILIDAD E IMPACTO** |
| Probabilidad: Alta.<br>Impacto: Moderado. |

| | |
|---|---|
| **EVIDENCIAS** | Evidencias/Documentos_AdquisicionSoftware |

Cuadro 67. Hallazgos AI1(2). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS AI2(1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas AA Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Adquirir y Mantener Software Aplicativo |
| **HALLAZGO** | | | |
| No existen procesos para comprobar la calidad de software que se adquiere con el fin de evaluar el cumplimiento de los requerimientos, políticas de adquisición y soporte de procedimientos que soportan el funcionamiento de la entidad. | | | |

| **CONSECUENCIAS** | |
|---|---|
| La falta de un proceso de verificación de requisitos del software puede llevar a la desconfianza en el funcionamiento del software y a dudar de su calidad, debido a la carencia de estudios y análisis previos de requerimientos, ya que el software debe satisfacer necesidades establecidas o implícitas de la institución. | |
| **RECOMENDACIONES** | |
| Implantar un procedimiento de medición de calidad de software teniendo en cuenta estos seis factores:<br><br>• Funcionalidad: ¿Las funciones requeridas están disponibles en el software?<br><br>• Confiabilidad: ¿Qué tan confiable es el software?<br><br>• Eficiencia: ¿Qué tan eficiente es el software?<br><br>• Usabilidad: ¿Es fácil de usar el software?<br><br>• Mantenibilidad: ¿Qué tan fácil de modificar es el software?<br><br>• Portabilidad: ¿Qué tan fácil es transferir el software a otro entorno?<br><br>El cumplimiento de los anteriores requisitos puede garantizar una mejor prestación del servicio de salud a los beneficiarios del servicio de salud de la IPSI Guaitara puesto que se están cumpliendo unos requisitos mínimos de calidad. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media.<br>Impacto: Moderado. | |
| **EVIDENCIAS** | Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/Entrevista_Audio/Entrevista2_PersonalEncargadoDeKardex.mp3<br>Evidencias/Entrevista_Audio/ Entrevista_PersonalEncargadoDeKardex.mp3 |

Cuadro 68. Hallazgos AI2. [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS AI4 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Facilitar la Operación y el Uso |

**HALLAZGO**

No existen manuales de funcionamiento de software, que indique la manera de realizar la transferencia de conocimiento.

Falta de documentación de registro de fallos en el software INFO-SALUD, como bitácora de errores.

No se tiene documentados los mensajes de alerta que utilizan códigos de error y tecnicismos que no representan claridad o ayuda para los empleados a la hora de resolver una falla.

**CONSECUENCIAS**

La falta de documentación técnica del software obliga a la entidad a tener una alta dependencia del ingeniero desarrollador, ya que él es el único que conoce a fondo el funcionamiento del software, por tal razón al presentarse inconvenientes es la única persona que puede ayudar a restablecer el servicio.

Al no existir un documento de comunicación técnica que brinde asistencia a los operarios que usan el software, la entidad puede estar siempre dependiente y amarrada del personal conocedor de procedimientos técnicos y operacionales del software.

La no existencia del manual puede generar inconsistencias en el manejo del software y puede perjudicar al personal reemplazante o el nuevo personal.

El personal encargado del soporte técnico del software no tiene la posibilidad de guiarse ante dudas o inconvenientes con el software ya que no posee las especificaciones de diseño de la base de datos y del funcionamiento del software en general.

| **RECOMENDACIONES** | |
|---|---|
| Solicitar al ingeniero desarrollador los manuales técnicos del software que contenga:<br><br>• Esquema de diseño de la base de datos donde se describa el tipo de los datos que hay en la base y la forma en que se relacionan.<br><br>• Guía de funcionalidad del software.<br><br>• Guía de instalación que contenga la información necesaria para implementar dicha aplicación además de las instrucciones para la puesta en marcha del sistema y las normas de utilización del mismo.<br><br>• Tener actualizado los manuales de los módulos de INFO-SALUD ante cualquier cambio o actualización.<br><br>• Dar a conocer los manuales técnicos y de operación al personal encargado del uso de los módulos del software INFO-SALUD.<br><br>• Documentación de conceptos acerca de mensajes y códigos de error<br><br>El personal encargado del área de sistemas de la IPSI Guaitara debe llevar un registro de fallos ocurridos de manera constante del software INFO-SALUD, para solicitar al proveedor aclaración sobre los mismos, así como también correcciones y soluciones. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Moderado. | |
| **EVIDENCIAS** | Evidencias/ /Evidencias/ANEXO D. Entrevista Audio/Entrevista_Aux_Atención_Usuario.mp3 Evidencias/ANEXO D. Entrevista Audio/Entrevista_AuxiliarHigieneOral.mp3 Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3 Evidencias/ANEXO G. Imágenes de pruebas |

Cuadro 69. Hallazgos AI4. [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS AI6 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Administrar Cambios |

**HALLAZGO**

No existe una política formal que permita el análisis, implementación y seguimiento de cambios requeridos en el aplicativo informático INFO-SALUD.

No existen procesos de revisión para garantizar la implantación completa y el correcto funcionamiento de las actualizaciones.

No se tiene documentación para operarios finales que lo guie en el manejo del software cuando se ha realizado cambios en algún módulo.

El proveedor implementa cambios en el software sin tener en cuenta las necesidades de la IPSI Guaitara

**CONSECUENCIAS**

La falta de planes y procedimientos para implementación de cambios en el software genera desorden y pérdida de tiempo al no priorizar las actualizaciones a realizar, falta de documentación y capacitación a los empleados, lo que puede ocasionar lentitud a la hora de realizar sus labores ya que no se puede conocer a plenitud el cambio realizado.

**RECOMENDACIONES**

Implementar un plan de procesos de actualizaciones de software, en el cual se analicen los cambios que la institución necesita que se realicen al software; este plan de procedimientos de actualizaciones tiene como objetivo identificar los cambios que necesita el software para cumplir con todos los requisitos de funcionalidad y eficiencia de la institución.

El proceso de actualizaciones se deberá especificar aspectos como:

- Evaluar, priorizar y autorizar cambios

| |
|---|
| • Llevar un control de cambios.<br>• Garantizar que el cambio quede bien implantado.<br>• Revisión y Aprobación. |
| **PROBABILIDAD E IMPACTO** |
| Probabilidad: Medio.<br>Impacto: Moderado. |

| | |
|---|---|
| **EVIDENCIAS** | Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3<br>Evidencias/ANEXO F.<br>Entrevistas_Preguntas_Cerradas/Gráficos de Resultados<br>Entrevistas Ipsi Guaitara |

Cuadro 70. Hallazgos AI6. [1]

| | | |
|---|---|---|
| | **HALLAZGOS** | **REF** |
| | | HDIS AI7 (1) |

| | | | |
|---|---|---|---|
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Instalar y Acreditar Soluciones y Cambios |
| **HALLAZGO** | | | |
| No se ha establecido un entorno de pruebas informáticas donde se pueda evaluar niveles de seguridad, controles internos, calidad de datos y cargas de trabajo del software INFO-SALUD. | | | |
| **CONSECUENCIAS** | | | |
| Al no llevar a cabo pruebas de rendimiento de las aplicaciones informáticas, se pueden generar errores en tiempo de ejecución durante su uso empresarial e incertidumbre acerca de su desempeño debido a desconocimiento de | | | |

| | |
|---|---|
| condiciones de carga, seguridad, compatibilidad, usabilidad, disponibilidad, entre otros. | |
| **RECOMENDACIONES** | |
| Establecer un plan de procedimientos de ejecución de pruebas informáticas, con el fin de evaluar el rendimiento de la aplicación en un entorno controlado, que debe ser una réplica del entorno informático implementado en la institución, logrando así probar la aplicación con datos de beneficiarios virtuales simulados, marcos automatizados y datos de prueba que se pueden editar en cualquier momento, con el propósito de examinar la aplicación bajo diferentes condiciones de carga, que permita garantizar el adecuado funcionamiento del software que funciona en línea.<br><br>El plan de ejecución de pruebas debe tener en cuenta los siguientes aspectos:<br><br>• Requerimientos de pruebas a ejecutar.<br>• Registro de “no conformidades” identificadas<br>• Ejecución de actividades de pruebas definidas en el plan de pruebas.<br>• Reporte de hallazgos.<br>• Identificación de acciones de mejoramiento (Retroalimentación). | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media.<br>Impacto: Catastrófica. | |
| **EVIDENCIAS** | Evidencias/ANEXO F.<br>Entrevistas_Preguntas_Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3<br>Evidencias/Entrevista_Audio/Entrevista2_IngSistemas.mp3 |

Cuadro 71. Hallazgos AI7(1). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS AI7 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Instalar y Acreditar Soluciones y Cambios |
| **HALLAZGO** | | | |
| No existen documentos de aceptación final del software después de haber realizado la evaluación de requerimientos. | | | |
| **CONSECUENCIAS** | | | |
| No existen documentos formales en donde se ratifique la realización de pruebas sobre el software, resultados que estas arrojaron ni un documento donde los encargados de evaluar los requerimientos del software acepten el cumplimiento de todos los requisitos y requerimientos.<br><br>La carencia de un plan de desarrollo de software que integre las actividades de pruebas de aceptación, genera incertidumbre, ya que se desconoce el alcance del sistema informático y por lo tanto no puede garantizar la continuidad de los servicios soportados por el software, ni la completa abstracción de los formatos que los operarios necesitan para lograr la buena y completa prestación de servicios a los beneficiarios. | | | |
| **RECOMENDACIONES** | | | |
| Formalizar la aceptación de software, con el fin de evaluar que el producto cumpla con los estándares necesarios y que a la vez satisfaga a los operarios de acuerdo a los requerimientos que se plantearon.<br><br>El objetivo principal de la legalización de aceptación, es validar que un sistema informático cumpla con el requerimiento esperado y permitir a los operarios de los módulos de INFO-SALUD su aceptación, desde el punto de vista de su funcionalidad y rendimiento con el fin de asegurarse que el sistema informático implementado cumple con los requisitos. | | | |
| **PROBABILIDAD E IMPACTO** | | | |
| Probabilidad: Media.<br>Impacto: Media. | | | |
| **EVIDENCIAS** | Evidencias/Documentos_AdquisicionSoftware<br>Evidencias/Entrevistas_Audio/Entrevista_DirectorAdministra.mp3 | | |

Cuadro 72. Hallazgos AI7(2). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS DS3 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Adquirir e Implementar | **PROCESO** | Instalar y Acreditar Soluciones y Cambios |

**HALLAZGO**

La base de datos informática de la empresa se encuentra almacenada en Microsoft Access 2010, una herramienta de diseño e implementación de aplicaciones de base de datos, siendo un factor de cuidado, debido a las características que este software presenta; como por ejemplo el tamaño máximo del archivo de la base de datos[99].

El método utilizado para compartir la base de datos de Microsoft Access es a través de una carpeta compartida en red, siendo un método que genera dificultad en la prestación del servicio debido a la caída constante de la base de datos utilizada por el software INFO-SALUD.

La base de datos de Microsoft Access utilizada en la IPSI Guaitara presenta protección por contraseña con un bajo nivel de seguridad.

No se hace un seguimiento evaluativo a la capacidad, desempeño y fallas que presenta el software relacionado con la base de datos Microsoft Access.

**CONSECUENCIAS**

Las especificaciones técnicas que Microsoft Access, comparadas con otros gestores de base de datos como por ejemplo: Microsoft SQL Server, PostgreSQL o MySQL, implican que hay factores a tener en cuenta como por ejemplo:

- Escalabilidad, capacidad para adaptarse a un número de usuarios y transacciones cada vez mayor, sin perder calidad en los servicios y su

[99] Soporte Microsoft, Especificaciones de Access 2010, https://support.office.com/es-hn/article/Especificaciones-de-Access-2010-1e521481-7f9a-46f7-8ed9-ea9dff1fa854#bmaccessdb [Consulta: 10 Enero 2015]

desempeño, lo cual con Microsoft Access no se puede alcanzar debido al límite de 2 Gb que tiene de almacenamiento (caractstica definida por el soporte de Microsoft en la sección “Especificaciones de Access 2010”), lo que implica que se debe pensar en la migración a otro gestor de base de datos que soporte un mayor tamaño en la base de datos.

- Licenciamiento, el pago de la Licencia de Microsoft Access debe ser anual a diferencia y teniendo en cuenta que no se crea un archivo compilado .EXE, se debe tener instalado en cada computador que necesite consultar la base de datos, por ello los costos por pago de licencia se incrementan.

La conexión con la cual se está compartiendo el archivo de Microsoft Access en el servidor no es la ideal, debido a que se está compartiendo en una carpeta de red y teniendo en cuenta las especificaciones que Microsoft da al tener este tipo de conexión “La confiabilidad y la disponibilidad pueden convertirse en problemas si hay varios usuarios simultáneos”[100] como es el caso en la IPSI Guaitara donde el software INFO-SALUD recibe solicitudes de varios equipos clientes al mismo tiempo y corre el riesgo de caída en el servicio, lo que implica dejar de registrar información en el software y demoras en tiempos de atención a beneficiarios.

La seguridad de los datos en una entidad como la IPSI Guaitara debe ser alta, lamentablemente el archivo de la base de datos almacenada en Access solo se encuentra protegida por medio de un password con un nivel bajo de seguridad y permisos por tabla o consulta que no garantizan protección alguna, estas implicaciones son un riesgo alto que no garantizan la seguridad de la información.

El no llevar un seguimiento evaluativo a las fallas de la base de datos, representa riesgo en el funcionamiento del software INFO-SALUD, debido a la dependencia directa con la información manejada en la base de datos, el desconocimiento del desempeño actual y la calidad de los datos que se ingresan.

**RECOMENDACIONES**

Se hace necesario solicitar al proveedor del software INFO_SALUD, la migración a un sistema gestor de base de datos como: Microsoft SQL Server, MySQL u Oracle que garantice seguridad y continuidad en la prestación del servicio.

[100] Soporte Microsoft , Formas de compartir una base de datos de Access, https://support.office.com/es-hn/article/Formas-de-compartir-una-base-de-datos-de-Access-2c24eb08-bee1-453e-be8e-455f847c5c74 [Consulta: 10 Enero 2015]

| | |
|---|---|
| Una medida para continuar utilizando Microsoft Accces a corto plazo hasta realizar la migración a otro gestor de base de datos con mejores características de funcionalidad y seguridad, es modificar el tipo de conexión que se tiene, el soporte de Microsoft en la sección "Dividir una base de datos[101]", detalla que una opción para optimizar el funcionamiento de Access es dividir la base de datos en dos partes, una denominada Back-End, es la que contiene las tablas exclusivamente y otra, llamada Front-End, que es la que contiene el resto de objetos de Access: formularios, consultas, informes, macros, módulos. Con ese tipo de conexión se logra aumento de rendimiento y velocidad de respuesta de la base de datos.<br><br>Implementar políticas de seguridad física y lógica, con intención de proteger la base de datos que se tiene en el momento, debido a su alta vulnerabilidad teniendo en cuenta la existencia de software que permite obtener la contraseña de un archivo de Microsoft Access.<br><br>El personal encargado del área de sistemas de la IPS Indígena Guaitara, debe llevar un registro de fallos ocurridos de manera constante en la base de datos Access que maneja el software INFO-SALUD, para solicitar al proveedor aclaración sobre los mismos, así como también correcciones y soluciones. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media.<br>Impacto: Media. | |
| **EVIDENCIAS** | Evidencias/ANEXO H. Videos de Pruebas/demostracion_accespv.mp4<br>Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/entrevista ingeniero (1)<br>Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/entrevista ingeniero (2)<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 |

Cuadro 73. Hallazgos DS3. [1]

[101] Soporte Microsoft , Formas de compartir una base de datos de Access, https://support.office.com/es-es/article/Dividir-una-base-de-datos-3015ad18-a3a1-4e9c-a7f3-51b1d73498cc [Consulta: 20 Septiembre 2015]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS DS4 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y Dar Soporte | **PROCESO** | Planes de Continuidad de TI |

**HALLAZGO**

No existen planes formales de contingencia efectivos orientados a la recuperación del sistema informático, donde se consideren requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los datos y servicios.

Al presentarse una falla en el software, los operarios tienen como plan de contingencia (informal) continuar con todos los registros de datos en hojas de cálculo o de forma manual, mientras se reestablece el servicio.

No se llevan a cabo sesiones de entrenamiento donde se explique al personal operario el procedimiento a realizarse en caso de interrupciones fortuitas.

**CONSECUENCIAS**

La falta de un plan de contingencia formal expone al sistema informático a fallas o interrupciones que harán que la IPS Indígena Guaitara deje de prestar un servicio de calidad a sus beneficiarios o puede desestabilizar el buen funcionamiento de la institución.

La ausencia de un plan de contingencia formal orientado a la recuperación del sistema informático, causa desinformación en los operarios, quienes no sabrán que decisiones tomar en caso de fallas y que acciones seguir cuando el sistema haya sido restaurado.

La falta de plan de contingencia cuando existen fallas en el software INFO-SALUD genera desorden a la hora de llevar los procesos de manera alternativa, llevando información en diferentes formatos (documentos escritos, plantillas de Word, Excel).

La ausencia de actividades o tareas de reanudación de servicio genera falta de integridad en la información debido a que los operarios del software INFO-

| | |
|---|---|
| SALUD, no actualizan la información que han llevado en diferentes formatos ocasionando riesgo de pérdida de información. | |
| **RECOMENDACIONES** | |
| Definir un plan de contingencias que especifique las acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen el Sistema informático de la IPS Indígena Guaitara, que permita restituir oportunamente los servicios de la organización ante la eventualidad de caída del sistema, ya sea de forma parcial o total y que puede afectar la prestación del servicio.<br><br>El plan de contingencia es una herramienta que ayudará a que los procesos críticos de la institución continúen funcionando a pesar de una posible falla en los sistemas computarizados; es un plan que puede permitir a la organización seguir prestando sus servicios a los beneficiarios.<br><br>Los planes de contingencia deben actualizarse, corregirse, y mejorarse constantemente con el fin de mantener la eficiencia, eficacia y estabilidad del sistema informático. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoAuditor.mp3 Evidencias/ANEXO D. Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Atención_Usuario.mp3 Evidencias/ANEXO D. Entrevista_Audio/Entrevista_Coordinacion_Facturacion.mp3 Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Facturación.mp3 |

Cuadro 74. Hallazgos DS4. [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS DS5(1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y Dar Soporte | **PROCESO** | Plan de Seguridad de TI |

**HALLAZGO**

No existe un plan de seguridad informático que garantice la protección de la información digital.

**CONSECUENCIAS**

Al no existir un plan de seguridad TI, la institución puede ser vulnerable a diferentes amenazas que pueden causar fallas en la prestación del servicio de salud a sus beneficiarios, entre estas amenazas están virus informáticos, pérdida o inconsistencia en la información, daños o pérdidas irreversibles de los activos hardware y software entre otros.

**RECOMENDACIONES**

Desarrollar un plan de seguridad informático para afrontar riesgos a los que se puede ver abocados el sistema informático de la entidad, en el cual se identifiquen los activos de software y hardware que deben protegerse, de forma que permitan la estabilidad de la institución.

La política de seguridad debe identificar posibles amenazas como:

- Violaciones a la seguridad y el impacto que tendrían si ocurrieran
- Amenazas externas como virus, ataques de hackers, retaliaciones de ex-empleados
- Amenazas internas son muy peligrosas y costosas ya que el infractor tiene mayor acceso y conocimiento para saber dónde reside la información sensible e importante para la institución

El plan de seguridad deberá evaluar los riesgos calculando la probabilidad de que ocurran ciertos sucesos y determinar cuáles tienen el potencial para causar más daño. Él va más allá de lo estrictamente monetario, dado que los activos tienen un valor agregado, tal es caso de los datos, la privacidad, responsabilidad legal, etc.

| | |
|---|---|
| Se debe asignar las responsabilidades correspondientes al personal encargado de la seguridad de la información digital, este personal debe saber identificar las amenazas potenciales que afecten al sistema informático.<br><br>Realizar copias de seguridad de las bases de datos informáticas regularmente, con el fin de salvaguardar la información digital, la cual es el activo más importante de la institución de esta manera se la puede proteger de posibles infecciones del sistema informático por virus y malware, apagados incorrectos de los equipos, daños causados por los operarios al borrar accidentalmente información entre otros. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Media.<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_IngSistemas.mp3 |

Cuadro 75. Hallazgos DS5(1). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS DS5 (2) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y Dar Soporte | **PROCESO** | Plan de Seguridad de TI |
| **HALLAZGO** | | | |
| Existen controles de usuario y contraseña para la identificación de cada operario de INFO-SALUD, pero no se utilizan estas cuentas de usuario. Se maneja una cuenta de usuario general con contraseña 1, por ejemplo: Usuario: CHILCOS Contraseña: 1 ó Usuario: USUARIO Contraseña: “1”. | | | |
| **CONSECUENCIAS** | | | |
| Los operadores de INFO-SALUD deben hacer uso de las cuentas de usuario creadas, ya que al utilizar una cuenta general no se podrá evaluar la identidad de los empleados que han utilizado el sistema informático; ni hacer un seguimiento a las actividades realizadas en el software; no se puede autenticar que personas han realizado cambios que pueden ser mal intencionados o por error; no se podrá establecer que funcionario fue el responsable. | | | |

| | |
|---|---|
| Los operarios y funcionarios que tienen acceso al sistema informático y utilizan contraseñas de bajo nivel de seguridad son un riesgo para la institución, ya que personas no autorizadas podrían ingresar al aplicativo y alterar o eliminar la información de las bases de datos informáticas; además se está vulnerando el derecho a la privacidad de los beneficiarios, ya que su historial médico está expuesto por fallas en la seguridad. | |
| **RECOMENDACIONES** | |
| Realizar periódicamente capacitación a los operadores del sistema informático en temas de seguridad, ya que se evidencia desconocimiento en este aspecto; es de vital importancia proporcionar lineamientos para que operarios utilicen las cuentas de usuario creadas por el ingeniero de sistemas y concientizar a los operarios que las claves deben ser complejas y no se deben divulgar, para garantizar la seguridad de la información.<br><br>Generar una cultura de seguridad informático, indicando que es conveniente cambiar la contraseña periódicamente para que el sistema informático sea más seguro, consistente e íntegro. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/Evidencias/ANEXO G. Imágenes de pruebas<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO E. Entrevistas_Preguntas_Abiertas |

Cuadro 76. Hallazgos DS5(2). [1]

| | | | |
|---|---|---|---|
| | **HALLAZGOS** | | **REF** |
| | | | HDIS DS5 (3) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y Dar Soporte | **PROCESO** | Plan de Seguridad de TI |
| **HALLAZGO** | | | |
| No existen permisos restringidos de acceso de usuario al sistema informático, todos los operarios pueden acceder a las funciones de otros empleados, por | | | |

| | |
|---|---|
| ejemplo el personal odontológico puede ingresar a las funciones e historias de clínicas de medicina general sin restricciones y viceversa. | |
| **CONSECUENCIAS** | |
| Cualquier operario puede visualizar, editar o eliminar la información digital a las funciones de otros operarios, generando así falta de integridad en la información digital.<br><br>No existe privacidad de los datos digitales de los beneficiarios, ya que sus historias clínicas pueden ser visualizadas por cualquier funcionario de la IPS, dado que no existe una política interna para la administración informática de grupos y permisos de usuario. | |
| **RECOMENDACIONES** | |
| Establecer procedimientos informáticos de cuentas de usuario, en donde se debe identificar:<br><br>• Los registros digitales a los cuales los operarios deben tener acceso.<br><br>• Los datos que se deben negar a otros operarios.<br><br>• Los datos que pueden ser compartidos<br><br>Estos procedimientos deben aplicarse a todos los operarios, incluyendo administradores (usuario privilegiado).<br><br>La política de administración informática de permisos debe establecer grupos para los empleados encargados de los módulos de INFO-SALUD y los respectivos derechos de acceso, con el fin de restringir y establecer perfiles de acceso de los operarios a archivos digitales para visualización de contenidos o modificación; incrementando así la privacidad de los operarios y evitar uso inadecuado de la información personal de los beneficiarios. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO D. Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_Aux_Atención_Usuario.mp3<br>Evidencias/ANEXO D. Entrevistas_Audio/Entrevista_AuxiliarHigieneOral.mp3 |

Cuadro 77. Hallazgos DS5(3). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| . | | | HDIS DS5 (4) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar y Dar Soporte | **PROCESO** | Plan de Seguridad de TI |
| **HALLAZGO** | | | |
| No existen medidas preventivas, detectivas y correctivas en la institución para proteger los sistemas informáticos y la tecnología que respalda este sistema contra malware.<br><br>Los operarios del sistema informático de la institución no conocen medidas de prevención que se deben usar sobre los equipos de cómputo para evitar infecciones informáticas. | | | |
| **CONSECUENCIAS** | | | |
| Puede haber pérdida de información digital, daños en el hardware y/o software o mal funcionamiento y lentitud en el procesamiento de datos debido a daños o ataques al sistema informático, ocasionado por software malicioso debido a falta de controles en el acceso a páginas no autorizadas de internet por falta de software antivirus no instalados o actualizados en los equipos. | | | |
| **RECOMENDACIONES** | | | |
| Implementar políticas de comunicaciones y navegación segura en Internet.<br><br>La IPS Indígena Guaitara debe adquirir software de protección que detecten y eliminen amenazas de software para disminuir el riesgo de daño al sistema informático.<br><br>Los empleados deben tener en cuenta aspectos de seguridad informática, para evitar la infección del sistema informático de la institución. | | | |
| **PROBABILIDAD E IMPACTO** | | | |
| Probabilidad: Alta.<br>Impacto: Catastrófico. | | | |
| **EVIDENCIAS** | Evidencias/Entrevista Audio/Entrevista_IngSistemas.mp3<br>Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas/Gráficos de Resultados Entrevistas Ipsi Guaitara | | |

Cuadro 78. Hallazgos DS5(4). [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS DS7 (1) |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar Y Dar Soporte | **PROCESO** | Educar y Entrenar a los Operarios |

**HALLAZGOS**

No se brinda capacitación continua a los operarios del sistema informático, la última capacitación formal fue impartida en el año 2010.

No existen planes que permitan identificar las necesidades de entrenamiento que tienen empleados encargados de operar los módulos del software, ya que durante este trabajo se evidenció la necesidad de cursos de informática básica para los empleados.

El proveedor del software INFO-SALUD no hizo entrega de manuales de usuario a la IPSI Guaitara y no se tiene una normativa de operación. Solamente entrego videos de algunas aplicaciones en donde se detalla que se tiene opciones desactualizadas.

El proveedor del software INFO-SALUD no hizo entrega de manuales de funcionamiento en donde se defina funciones y procedimientos de cada módulo, lo que implica disminución en la productividad y el cumplimiento de los controles clave, tales como las medidas de seguridad.

**CONSECUENCIAS**

Al no existir una capacitación continua del manejo, operación o cambios del software INFO-SALUD, se corre el riesgo de incremento en errores, por parte de los operarios que no recibieron capacitación y genera dependencia, puesto que es poco el personal que conoce en gran medida el funcionamiento y operación del software.

Al desconocer el funcionamiento de funciones y procedimientos se corre el riesgo de incurrir en deficiencia en la calidad de información digital almacenada.

La no existencia de manuales de usuario y procedimientos del software hacen

| | |
|---|---|
| que la dependencia hacia el proveedor del software sea alta, incurriendo en gastos adicionales por fallos que podrían ser evitables. | |
| **RECOMENDACIONES** | |
| Plantear cronogramas de capacitación y planes de entrenamiento periódicos teniendo en cuenta cambios en el software que afecten la eficiente operación por parte de los empleados, esto contribuirá a evitar errores.<br><br>Organizar evaluaciones de desempeño para detectar posibles errores por desconocimiento de manejo de componentes del software.<br><br>Exigir al proveedor en futuras actualizaciones o adquisiciones de software, manuales de usuario y funcionamiento que permitan entender con mayor facilidad la funcionalidad y procedimientos de cada componente del software. | |
| **PROBABILIDAD E IMPACTO** | |
| Probabilidad: Alta.<br>Impacto: Catastrófico. | |
| **EVIDENCIAS** | Evidencias/ANEXO F.<br>Entrevistas_Preguntas_Cerradas/Gráficos de Resultados<br>Entrevistas Ipsi Guaitara<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoGeneral.mp3<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_MedicoAuditorl.mp3.mp3<br>Evidencias/ANEXO D.<br>Entrevistas_Audio/Entrevista_IngSistemas.mp3<br>Evidencias /Entrevista Audio/Entrevista_Aux_Facturación<br>Evidencias/Videos_Desarrollador<br>Evidencias/Instalacion_tesis_INFOSALUD.mp4 |

Cuadro 79. Hallazgos DS7. [1]

| | HALLAZGOS | | REF |
|---|---|---|---|
| | | | HDIS DS13 |
| **ENTIDAD AUDITADA** | **IPS INDÍGENA GUAITARA** | | |
| **OBJETO DE ESTUDIO** | Módulos de HistoriaNet, Citas Médicas, Facturación y Kardex del Software INFO-SALUD | | |
| **RESPONSABLES** | Mauricio Aza Arévalo – Mélanny Oviedo Mesías | | |
| **MATERIAL DE SOPORTE** | COBIT | | |
| **DOMINIO** | Entregar Y Dar Soporte | **PROCESO** | Administración de Operaciones. |
| **HALLAZGO** | | | |
| No existe un plan de soporte técnico o manejo, que permita conocer tiempos y procedimientos de mantenimiento en las dependencias, que permita prevenir fallas y dar una solución adecuada cuando existan problemas de hardware. | | | |
| **CONSECUENCIAS** | | | |
| En la IPSI Guaitara, las dependencias no tienen un manual de procedimientos ante un fallo en el hardware.<br><br>El desconocimiento de correctas prácticas de manejo de Hardware por parte de los operarios de la IPSI Guaitara hace vulnerable los equipos de cómputo. | | | |
| **RECOMENDACIONES** | | | |
| Realizar jornadas de capacitación dirigidas al personal que opera un equipo de cómputo enfocado en buenas prácticas de manejo de hardware y así generar cultura informática con el propósito de asegurar que los funcionarios utilicen de manera correctamente los recursos tecnológicos para el uso de las funciones.<br><br>Se debe tener un cronograma de mantenimiento preventivo del hardware en la institución, que contemple un correcto funcionamiento de todos los equipos de cómputo para así evitar entorpecer el funcionamiento normal del software y de otras áreas de la entidad que pueden generar interrupciones en las actividades.<br><br>Se recomienda la contratación de un auxiliar de soporte técnico en el área de sistemas que colabore en el soporte y mantenimiento del equipo de cómputo supervisado por el ingeniero de sistemas de la IPSI Guaitara. | | | |
| **PROBABILIDAD E IMPACTO** | | | |
| Probabilidad: Media<br>Impacto: Medio | | | |
| **EVIDENCIAS** | Evidencias/ANEXO D. Entrevista Audio/Entrevista_CoordinadorDeFacturación.mp3<br>Evidencias/ANEXO D. | | |

Cuadro 80. Hallazgos DS13

**3.2.7 Informe general de la auditoría**. El software INFO-SALUD, fue sometido a una auditoria informática, para evaluar los módulos que hacen parte de este aplicativo, tanto en entradas, procesos y salidas de datos, de igual manera en lo referente a seguridad de la información procesada en el software.

Después de realizar las pruebas y la verificación de procedimientos realizados sobre los módulos que conforman el software INFO-SALUD se relacionan algunos aspectos favorables generales extraídos del informe de la presente auditoría.

La auditoría se realizó con buena disposición por parte del personal encargado del manejo de los módulos del software.

El software posee un buen proceso de generación de informes, lo que permite la automatización de los procesos, agilizando la generación de informes institucionales requeridos por las entidades de control como la EPS y la Secretaria departamental de salud, minimizando trabajos operativos y estandarizar los procesos.

Cada proceso para generación de informes tiene incluido filtros, lo que facilita la recolección de datos y su correcto procesamiento para campañas extramurales de promoción y prevención.

INFO-SALUD Facilita el proceso de asignación de citas médicas mediante la generación de una agenda médica, por medio de la cual se tiene acceso rápido a datos generales de los pacientes que solicitan una cita médica, estas herramientas que reduce el tiempo necesario para gestionar cita.

El aplicativo informático genera reportes que brindan información sobre los datos capturados en la agenda, como asistencia de pacientes y carga de trabajo por profesional de la salud.

El módulo de citas médicas del aplicativo INFO-SALUD, permite controlar expedientes médicos digitalizados (historias clínicas, situación del paciente y su familia, entre otros) de manera ágil.

El software INFO-SALUD provee búsquedas fáciles por medio de ayudas por códigos y nombre de diagnósticos y medicamentos que permiten agilizar la práctica clínica.

El software en referencia, permite manejar formularios, en el cual se realiza un seguimiento de los controles correspondientes a un paciente. Al diligenciar un nuevo control se pueden ingresar antecedentes, examen físico, formulación de laboratorio, formulación de medicamentos, realización de procedimientos, Imagenología, selección de diagnóstico, datos del acompañante, y diligenciar

notas de enfermería correspondientes al beneficiario, lo que permite llevar un seguimiento completo de su situación médica.

El módulo de Facturación del aplicativo informático INFO-SALUD, permite llevar un control de las unidades existentes en las sedes de la institución facturando de acuerdo a la parametrización realizada en el momento de crear los contratos, esta información puede ser modificada de acuerdo a las necesidades de cada operario.

Sin embargo el trabajo de auditoría permitió identificar hallazgos, en donde se evidencian oportunidades de mejoramiento para las cuales, el equipo auditor formula recomendaciones y sean tenidas en cuenta por los entes administrativos de la IPS Indígena Guaitara que permiten alcanzar mejoras en los procesos en donde el aplicativo informático INFO-SALUD es parte activa.

**Respecto a la Arquitectura de la Información.**

**Hallazgos**

- No se tiene un diccionario de datos donde especifique el tipo de datos que se manejan en la base de datos e indique si es de entrada y/o salida[102].
- No existen diagramas de flujo de los módulos del software INFO-SALUD[103].
- No existen esquemas de diseño donde se detallen la lógica de los procesos que se administran desde el software INFO-SALUD[104].

**Consecuencia**

- La inexistencia de documentación, diagramas de funcionamiento y diccionario de datos donde se especifican los detalles del aplicativo informático, genera dificultad a la hora de resolver fallas o realizar mantenimiento a la aplicación por parte de los ingenieros encargados de administrar los procesos del aplicativo informático INFO-SALUD.

**Recomendaciones**

- Documentar el diccionario de datos de los módulos del software INFO-SALUD.

[102] Hallazgos PO2(1)
[103] Hallazgos PO2(3)
[104] Hallazgos PO2(3)

- Incorporar dentro del diccionario de datos, la clasificación de tipos de operarios, los niveles de acceso y las restricciones para el ingreso de los mismos.

- Tener actualizado el diccionario de datos ante cambios o implementación de nuevas funcionalidades.

**Hallazgos**

- No existen esquemas de clasificación de la información basados en el nivel de confidencialidad de los datos administrados por la aplicación informática[105].

- No existe un plan de seguridad en los procesos que se manejan en el software INFO-SALUD, que garantice la integridad y consistencia de los datos almacenados en formato electrónico.

- No existen esquemas donde se definan niveles apropiados de seguridad y de controles de protección de datos, en especial los controles de acceso[106].

**Consecuencia**

- La falta de esquemas documentados de clasificación de la información y procesos llevados en el aplicativo informático, no permite identificar la información relevante y de carácter privado, incurriendo en riesgos de perdida de privacidad de la información, integridad e inconsistencia en los datos almacenados.

**Recomendaciones**

- Diseñar un plan de administración de seguridad informática que proporcionen los controles de seguridad suficientes que protejan los activos de información digital.

- Tener adecuadas políticas y procedimientos relacionados con la seguridad de los activos informáticos; considerando que la información debe estar clasificada según la necesidad de acceso.

- Verificar que los controles de acceso al sistema informático garanticen que la información sea asequible y utilizable sólo por el personal autorizado.

---

[105] Hallazgos PO2(1)
[106] ibíd.
[106] Hallazgos PO2(3)

- Revisar y evaluar el desempeño (eficiencia y eficacia) del plan de seguridad informática que se vaya a implementar.

**Hallazgos**

- No existe un manual de instalación del aplicativo informático, donde se especifiquen requerimientos del software y hardware necesarios para su funcionamiento[107].

- No existe documentación en la que se describa la configuración y funcionamiento del software INFO-SALUD[108].

- No existen diagramas de flujo de datos y/o pseudocódigo de las partes de los módulos y sus especificaciones[109].

**Consecuencias**

- El desconocimiento de configuración y funcionamiento debido a la inexistencia de documentación que sirva de referencia, genera dependencia hacia el proveedor del aplicativo informático debido a que solo él, conoce aspectos de configuración y funcionamiento que son necesarios para eventuales correcciones o mantenimientos.

- La falta de documentación técnica donde se especifiquen diagramas de flujo generan dificultas en la comprensión del funcionamiento de los módulos que conforman el aplicativo informático Info-Salud, dificultando así la implementación de procesos de mantenimiento y planes de corrección de errores.

**Recomendaciones**

- En futuras negociaciones solicitar al ingeniero proveedor del aplicativo informático documentación en donde se incluya documentación de soporte como manual de diseño, manual de usuario y manual técnico.

- En el contrato de renovación del aplicativo informático INFO-SALUD o adquisición de otro aplicativo informático, la IPSI GUAITARA debe incluir cláusulas en donde se especifiquen:

    - Requerimientos Funcionales de la IPSI GUAITARA

[107] ibíd.
[108] ibíd.
[109] ibíd.

- Condiciones técnicas y especificas del aplicativo informático
- Documentación de soporte
- Etapas y tiempos en la implementación del aplicativo informático en las fases de:
  - Planeación
  - Diseño
  - Configuración
  - Pruebas
  - Capacitación
  - Preparación
  - Estabilización

❖ Requerir que el aplicativo informático garantice la integridad de los datos mediante la implementación de:

- Reglas de normalización de datos
- Integridad referencial
- Validación de los datos

**Respecto a Procesos y Relaciones TI**

**Hallazgo**

❖ Existe mucha de dependencia del personal que posee conocimiento y tiene experiencia del manejo del aplicativo.

❖ No existen políticas de capacitación y manuales para que operarios nuevos aprendan a manejar el aplicativo informático[110].

**Consecuencias**

❖ La dependencia hacia personal con alto nivel de conocimiento en el aplicativo informático, pone al sistema informático en manos de pocas personas, siendo esto un riesgo, ya que si estas personas salen de la

[110] Hallazgos PO4

institución, esta podría verse afectada en el funcionamiento de sus procesos.

- Este personal especializado, con frecuencia posee la experiencia y el conocimiento no registrado de las modificaciones o el funcionamiento del aplicativo informático. La supervisión y el control de su trabajo resulta difícil debido a la dependencia excesiva hacia este tipo de personal.

**Recomendaciones**

- Identificar al personal con alto nivel de conocimiento de la aplicación informática Info-Salud con el fin de generar planes estratégicos y tácticos para la captura documental del conocimiento de este tipo de personal, compartir este conocimiento adquirido por la experiencia al personal recientemente vinculado.

- Implementar planes de capacitación para el personal nuevo, con el fin de mejorar la calidad y disminuir la dependencia de personal con experiencia.

- La entidad debe tener los manuales de funcionamiento de software actualizados y al alcance de todos los operarios del sistema informático ya que servirán de material de apoyo para el buen ejercicio de sus actividades.

**Respecto a Administrar Recursos TI**

**Hallazgos**

- No existe entrenamiento permanente del personal relacionado con el sistema informático[111].

- Se realizó una capacitación inicial en el año 2010, año en el que se adquirió el software, posterior a este fecha no se han realizado capacitaciones pese a las actualizaciones y cambios funcionales en los módulos del software INFO-SALUD[112].

- Dificultad de los empleados nuevos para llevar a cabo su trabajo, ya que no se ha realizado la capacitación necesaria.

- No existe un manual de funcionamiento del aplicativo informático que permita conocer su manejo.

[111] Hallazgos PO7(2)
[112] ibíd.

**Consecuencias**

- Debido a la falta de políticas de entrenamiento continuo, los empleados tienen menos probabilidades de completar las tareas de forma eficiente y efectiva.

- Puede causar traumas de tiempo en la prestación de los servicios de la Institución reduciendo drásticamente la buena imagen de esta.

- Una vez que la calidad en el servicio se reduce, se vuelve más difícil dedicar tiempo y dinero a la capacitación y al mantenimiento del aplicativo informático.

- A los empleados les toma más tiempo familiarizarse con el sistema informático con el que laboran debido a la no existencia de un manual de aplicativo informático.

**Recomendaciones**

- Establecer procesos periódicos de capacitación a los operarios de los módulos del software INFO-SALUD; esta capacitación debe incluir además de charlas acerca del funcionamiento del software, los manuales de usuario donde se especifique su funcionalidad.

- La capacitación debe ser obligatoria y permanente, dado que es un factor importante que ayuda a los operarios en el manejo del software INFO-SALUD, que puede dar como resultado una mejora en la prestación de servicio a los beneficiarios.

**Hallazgo**

- No existe documentación de control y registro de errores presentados en el software INFO-SALUD.

**Consecuencias**

- La falta de documentación técnica acerca del funcionamiento del aplicativo informático, registro de funcionalidades o medidas en caso de errores conlleva a procesos mal ejecutados por desconocimiento de las funcionalidades del aplicativo INFO-SALUD.

- Los procesos informales de capacitación de personal, generan falta de bases sólidas en cuanto a la funcionalidad técnica del aplicativo informático INFO-SALUD.

**Recomendación**

- Implementar procesos de gestión del conocimiento que promuevan la capacitación, evaluación, recuperación, preservación y aprovechamiento del conocimiento. Esto puede lograr experticia de los operarios encargados del manejo de los módulos del software INFO-SALUD en la institución, con el fin de generar una retroalimentación positiva en los procesos administrados por este aplicativo informático, eliminando así la dependencia del personal clave encargado del sistema informático en la organización.

**Hallazgo**

- No se toman medidas de seguridad informática, tales como eliminar privilegios de acceso al Software INFO-SALUD en el evento de terminación de contrato laboral del personal[113].

**Consecuencias**

- La falta de control en la administración de los privilegios de acceso para el ingreso al aplicativo INFO-SALUD, genera fallas en la seguridad de la información, ya que el personal que ha terminado el contrato con la institución aún tienen activos sus privilegios para ingresar a información confidencial que podrían modificar, esto puede causar inconsistencias, falta de veracidad de la información y riesgos de alteración.

**Recomendación**

- Establecer políticas generales para la gestión de seguridad del sistema informático que establezcan estrategias como:
  - Administración de cuentas de usuario
  - Administración de contraseñas de usuario
  - Verificación de usos de usuario, contraseñas y niveles de seguridad
  - Concientización a los operarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Mantener un archivo digital de auditoría o logs, donde se registren automáticamente todas las operaciones realizadas por los operarios; en caso de sospecha de falla en la seguridad, este archivo puede ser

[113] Hallazgos PO7(4)

consultado por personas de confianza autorizadas y capacitadas, y quienes deben ser diferentes a los operarios. El archivo digital de auditoría, permite conocer el autor y las acciones realizadas por los diferentes operarios, siempre y cuando cada operario maneje su propia cuenta de usuario y contraseña.

- ❖ Instituir estrategias para verificar el cumplimiento de los protocolos establecidos en el sistema informático, relacionadas con control de acceso, creación de usuario, administración de privilegios, autenticación de usuario y uso controlado de utilitarios del software INFO-SALUD.

- ❖ Una buena administración de la seguridad informática permitirá mayor control de las actividades de los operarios sobre el aplicativo INFO-SALUD.

**Respecto a Administrar Riesgos TI**

**Hallazgo**

- ❖ No existe plan de mitigación de riesgos cuando se presentan fallas en el software INFO-SALUD[114].

**Consecuencias**

- ❖ Cualquier entidad está expuesta al riesgo de interrupción del servicio por diversas causas, siendo las más frecuentes las relacionadas con fallas en los sistemas informáticos, el cual es uno de los ejes de la operatividad de una organización, puede ser vulnerable debido a riesgos informáticos y por lo tanto, se debe estar preparados para cualquier eventualidad. Por lo tanto, es pertinente crear y fortalecer una conciencia colectiva sobre la trascendencia del tema de recuperación en caso de desastres.

**Recomendación**

- ❖ Definir, implementar, probar y mantener un proceso para administrar la continuidad del servicio informático, que incluya elementos como:

    - Prevención y atención de emergencias
    - Administración de la crisis
    - Plan de contingencias
    - Capacidad de retorno a la operación normal

[114] Hallazgos PO9(2)

- El plan de contingencia orientado al aplicativo informático debe cumplir:

    - Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia

    - Ser conocido por todos los involucrados

    - Cubrir los siguientes aspectos: identificación de eventos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y retorno a las actividades normales

    - Efectuar de manera cronológica un diagnóstico sobre la situación de los sistemas informáticos que incluya análisis de riesgos y su variación en los niveles

    - Observar los protocolos y procedimientos establecidos para la protección de la información y garantizar la preservación de la memoria institucional.

**Respecto a Soluciones Automatizadas**

**Hallazgo**

- No hay procedimientos para especificar los requerimientos funcionales y técnicos del aplicativo que cubran las necesidades de la organización[115].

**Consecuencias**

- Debido a la falta de implementación de un proceso para la gestión de requerimientos hace que no estén desarrollados todos los procesos necesarios en la IPS Indígena Guaitara.

**Recomendaciones**

- Generar un proceso formal para la gestión de requerimientos y requisitos del sistema informático donde exista especificación de requerimientos informáticos funcionales y no funcionales descritos de manera concreta y consistente que permitan la atención completa a los beneficiarios de la institución.

- En el proceso de generación de requerimientos orientados al sistema informático deben establecer:

[115] Hallazgos AI1(1)

- Requerimientos del producto informático, en los que se especifique el comportamiento del software.

- Requerimientos de desempeño, donde se describen la rapidez de ejecución del sistema informático y el mínimo de memoria requerido para su funcionamiento.

- Requerimientos de fiabilidad que fijan la tasa de fallas, para que el sistema informático sea aceptable.

- Requerimientos organizacionales. Se derivan de las políticas y procedimientos existentes en la organización orientados al sistema informático.

- Requerimientos de entrega que especifiquen cuándo se entregará el producto informático y su documentación.

- Requerimientos externos. Se derivan de los factores externos al sistema informático y de su proceso de desarrollo.

- Requerimientos de Interoperabilidad que definen la manera en que el aplicativo informático INFO-SALUD interactúa con los otros sistemas de la organización.

**Hallazgo**

- No se realizó un estudio de factibilidad antes de la adquisición del aplicativo informático

**Consecuencias**

- La falta de planificación para la adquisición de un aplicativo informático puede generar inconsistencias debido a la imprecisión de los requerimientos necesarios para la organización y puede desmejorar el servicio que se presta a los beneficiarios de la entidad.

**Recomendación**

- Definir políticas formales de factibilidad para la adquisición de aplicativo informático en el cual se deben establecer las razones que amerita la adquisición de un nuevo sistema informático, capacidad técnica que implique la implantación del sistema en cuestión, así como estudio y análisis de costos, beneficios y el grado de aceptación que la propuesta genera en la Institución.

**Respecto a Adquirir y Mantener Aplicativo informático.**

**Hallazgo**

- No existen procesos para comprobar la calidad de aplicativo informático que se adquiere, con el fin de verificar el cumplimiento de los requerimientos, políticas de adquisición y soporte de procedimientos que soportan el funcionamiento de la entidad.

**Consecuencia**

- La falta de un proceso de verificación de requisitos de INFO-SALUD conlleva a la desconfianza en el funcionamiento del aplicativo informático y a dudar de su calidad, debido a la carencia de estudios y análisis previos de requerimientos.

**Recomendación**

- Implementar procedimientos de medición de calidad de aplicativo informático teniendo en cuenta factores como funcionalidad, confiabilidad, eficiencia, usabilidad, mantenibilidad y portabilidad:

- El cumplimiento de los anteriores requisitos puede garantizar una mejor prestación del servicio de salud a los beneficiarios del servicio de salud de la IPS Indígena Guaitara puesto que se están cumpliendo unos requisitos mínimos de calidad.

**Respecto a Facilitar la Operación y Uso**

**Hallazgo**

- No existen manuales de funcionamiento de software INFO-SALUD, que facilite la transferencia de conocimiento del aplicativo informático[116].

**Consecuencias**

- La falta de documentación técnica del software, obliga a la entidad a tener una alta dependencia del ingeniero desarrollador, ya que él es el único que conoce a fondo el funcionamiento del software, por tal razón al presentarse inconvenientes es la única persona que puede ayudar a restablecer el servicio.

[116] Hallazgos AI4

- La falta de manuales de usuario, genera inconvenientes a la hora de aplicar procesos de entrenamiento a los operarios de INFO-SALUD, ya que no existe documentación que pueda ser estudiada.

**Recomendación**

- Solicitar al Ingeniero desarrollador, los manuales técnicos del aplicativo informático INFO-SALUD que contenga:

  - Esquema de diseño de la base de datos que soporta el aplicativo informático, donde se describa el tipo de datos que se manejan y/o almacenan en las tablas y la forma en que se relacionan.

  - Guía de funcionalidad del aplicativo informático INFO-SALUD.

  - Guía de instalación, que contenga la información necesaria para implementar dicha aplicación informática, además de las instrucciones para la puesta en marcha del software INFO-SALUD y las normas de utilización del mismo.

  - Tener actualizados los manuales de los módulos de INFO-SALUD ante cualquier cambio o actualización.

  - Dar a conocer los manuales técnicos y de operación al personal encargado del manejo de los módulos del software INFO-SALUD.

**Respecto a Administrar Cambios**

**Hallazgos**

- No existe un protocolo formal que permita el análisis, implementación y seguimiento de cambios requeridos en el aplicativo informático INFO-SALUD[117].

- No existen procesos de revisión y control sistémico para garantizar la implantación completa y el correcto funcionamiento de las actualizaciones realizadas al aplicativo informático INFO-SALUD[118].

- No se tiene documentación para operarios finales con respecto al manejo de cambios en algún módulo del software INFO-SALUD[119].

[117] Hallazgos PO9(2)
[118] Hallazgos AI6
[119] Ibid.

- El proveedor realiza cambios en el software sin tener en cuenta las necesidades de la IPS Indígena Guaitara[120].

**Consecuencias**

- La falta de procedimientos para implementación de cambios genera desorden y pérdida de tiempo al no priorizar las actualizaciones a realizar, falta de documentación y capacitación a los empleados puede ocasionar lentitud a la hora de realizar sus labores, ya que no se puede conocer a plenitud el cambio realizado.

**Recomendaciones**

- Implementar un proceso de actualizaciones de software en el cual se analicen los cambios que la institución necesita y que se realicen al aplicativo informático INFO-SALUD; este procedimiento tiene como objetivo identificar los ajustes que necesita el software para cumplir con los requisitos de funcionalidad y eficiencia establecidos por la institución.

- En el proceso de actualizaciones del software INFO-SALUD se debe especificar aspectos como:

    - Evaluar, priorizar y autorizar cambios
    - Llevar un control de cambios
    - Garantizar que los cambios queden bien implantados
    - Revisión y aprobación de ajustes

**Hallazgos**

- La base de datos informática de la empresa se encuentra almacenada en Microsoft Access 2010, una herramienta de diseño e implementación de aplicaciones de base de datos, siendo un factor de cuidado, debido a las características que este software presenta; como por ejemplo el tamaño máximo del archivo de la base de datos[121].

- El método utilizado para compartir la base de datos de Microsoft Access es a través de una carpeta compartida en red siendo un método que genera

[120] Ibid.
[121] Soporte Microsoft , Especificaciones de Access 2010, https://support.office.com/es-hn/article/Especificaciones-de-Access-2010-1e521481-7f9a-46f7-8ed9-ea9dff1fa854#bmaccessdb [Consulta: 10 Enero 2015]

dificultad en la prestación del servicio debido a la caída constante de la base de datos utilizada por el software INFO-SALUD.

- La base de datos de Microsoft Access utilizada en la IPS Indígena Guaitara presenta protección por contraseña con un bajo nivel de seguridad.

**Consecuencias**

- Según las especificaciones técnicas Microsoft Access, no se puede superar el límite de 2 Gb que permite de almacenamiento, lo que implica falta de escalabilidad en la aplicación informática INFO-SALUD, por lo tanto la empresa no podrá registrar un gran número de beneficiarios ya que la bases de datos podría colapsar.

- Debido a las especificaciones técnicas de Microsoft, la forma como se realiza la conexión a la base de datos no es idónea, ya que se presentan problemas de actualización de datos cuando hay varios usuarios simultáneos.

- La base de datos almacenada en Access solo se encuentra protegida por medio de un password con un nivel bajo de seguridad y permisos por tabla o consulta que no garantizan protección alguna, estas implicaciones son un riesgo alto que no garantizan la seguridad de la información.

- El no llevar un seguimiento evaluativo a las fallas de la base de datos, representa un riesgo en el funcionamiento del software INFO-SALUD debido a la dependencia directa con la información manejada en la base de datos, el desconocimiento del desempeño actual y la calidad de los datos que se ingresan.

**Recomendaciones**

- Solicitar al proveedor del software INFO_SALUD, la migración a un sistema gestor de base de datos como: Microsoft SQL Server, MySQL u Oracle que garantice seguridad y continuidad en la prestación del servicio.

- Una medida para continuar utilizando Microsoft Accces a corto plazo hasta realizar la migración a otro gestor de base de datos con mejores características de funcionalidad y seguridad, es modificar el tipo de conexión que se tiene, el soporte de Microsoft en la sección “Dividir una base de datos ”, detalla que una opción para optimizar el funcionamiento de Access es dividir la base de datos en dos partes, una denominada Back-End, es la que contiene las tablas exclusivamente y otra, llamada Front-End, que es la que contiene el resto de objetos de Access: formularios,

consultas, informes, macros, módulos. Con ese tipo de conexión se logra aumento de rendimiento y velocidad de respuesta de la base de datos.

- Implementar políticas de seguridad física y lógica, con intención de proteger la base de datos que se tiene en el momento, debido a su alta vulnerabilidad teniendo en cuenta la existencia de software que permite obtener la contraseña de un archivo de Microsoft Access.

- El personal encargado del área de sistemas de la IPSI Guaitara, debe llevar un registro de fallos ocurridos de manera constante en la base de datos Access que maneja el software INFO-SALUD, para solicitar al proveedor aclaración sobre los mismos, así como también correcciones y soluciones.

**Respecto a Planes de Continuidad**

**Hallazgos**

- No existen planes formales de contingencia orientados al sistema informático, donde se consideren requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los servicios informáticos[122].

- Al presentarse una falla en el software, los empleados tienen como plan de contingencia (informal), continuar con los registros en hojas de cálculo o de forma manual.

- No se realizan sesiones de entrenamiento, donde se explique al personal operario, el procedimiento a realizarse en caso de interrupciones fortuitas en la prestación del servicio del sistema informático.

**Consecuencias**

- La falta de un plan de contingencia formal expone al sistema informático a fallas o interrupciones que harán que la IPSI deje de prestar un servicio de calidad a sus beneficiarios o puede desestabilizar el buen funcionamiento de la institución.

- La falta de plan de contingencia cuando existen fallas en el software puede generar desorden a la hora de llevar la información en diferentes formatos (documentos escritos, plantillas de Word, Excel) cuando no está funcionando el aplicativo.

[122] Hallazgo 19 HDSI

- La ausencia de actividades o tareas de reanudación de servicio genera falta de integridad en la información, debido a que los operarios del software INFO-SALUD no actualizan la información que han llevado en diferentes formatos, ocasionando riesgo de posible pérdida de información.

**Recomendaciones**

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen el Sistema de Informático de la IPSI, que permita restituir confiablemente los servicios informáticos de la organización ante la eventualidad de los procesos que se puedan paralizar, ya sea de forma parcial o total y que puedan alterar la prestación del servicio de salud.

- Definir un plan de contingencia que permita que los servicios de la entidad de salud continúen funcionando a pesar de una posible falla en el aplicativo informático INFO-SALUD; es decir, un plan que permita a la organización seguir prestando servicio a los beneficiarios.

- Los planes de contingencia deben actualizarse, corregirse, y mejorarse constantemente con el fin de verificar su eficacia y eficiencia.

**Respecto a Plan De Seguridad**

**Hallazgo**

- A pesar de que, existen registrados en el sistema informático cuentas de usuario y contraseñas para la identificación de cada operario de INFO-SALUD, estos controles de acceso no se utilizan adecuadamente por el contrario, se maneja una cuenta de usuario general con contraseña "1"[123].

**Consecuencias**

- Cualquier operario puede visualizar, editar o eliminar la información digital o ingresar a las funciones de otros operarios de la IPSI Guaitara, generando así falta de integridad en la información digital manejada por el aplicativo informático INFO-SALUD.

- No existe privacidad de los datos digitales de los beneficiarios, ya que sus historias clínicas pueden ser visualizadas por cualquier funcionario de la IPSI Guaitara, dado que no existe una política interna para la administración informática de grupos y permisos de usuario.

[123] Hallazgos DS5(2)

**Recomendaciones**

- Realizar una capacitación dirigida a los operadores del sistema informático en temas de seguridad, ya que se evidencia desconocimiento en este aspecto; es de gran importancia proporcionar lineamientos para que los operarios utilicen las cuentas de usuario creadas por el ingeniero de sistemas y explicar al personal encargado del manejo del aplicativo INFO-SALUD, que las claves deben ser seguras y no deben ser divulgadas para garantizar la seguridad de la información manejada por el aplicativo informático.

- Inhabilitar cuentas de operarios que ya no trabajen para la entidad o hayan sido reubicados.

- Cuando ingresen operarios nuevos a la entidad asignarles su propia cuenta y contraseña personalizada.

**Hallazgo**

- No existen permisos de acceso de usuario limitados o restringidos al sistema informático, cada operario puede acceder a todas las funciones del aplicativo, por ejemplo el personal odontológico puede ingresar a las funciones e historias de clínicas de medicina general y viceversa[124].

**Consecuencias**

- Cualquier operario puede visualizar, editar o eliminar la información digital a las funciones de otros operarios, generando así falta de integridad en la información digital.

- No existe privacidad de los datos digitales de los beneficiarios, ya que sus historias clínicas pueden ser visualizadas por cualquier funcionario de la IPS, dado que no existe una política para la administración informática de grupos y permisos de usuario

**Recomendaciones**

- Establecer procedimientos que permitan limitar o restringir paramétricamente las cuentas de usuario del aplicativo informático INFO-SALUD, donde se deben identificar los procesos a los que lo operarios deben tener acceso, los procesos que se deben restringir y qué información

[124] Hallazgos DS5(3)

debería ser compartida. Estos procedimientos deben aplicarse a todos los operarios, incluyendo administradores (usuario privilegiado).

- La política de administración de permisos orientados al sistema informático, debe establecer grupos y atributos para los empleados encargados del manejo de los módulos de INFO-SALUD y los respectivos derechos de acceso, con el fin de asegurar el acceso a archivos digitales para visualización de contenidos o edición, mejorando así la privacidad de datos y uso inadecuado de la información personal de los beneficiarios.

**Hallazgos**

- No existen en la institución medidas preventivas, detectivas y correctivas, para proteger los sistemas informáticos contra software malicioso[125].

- Los operarios del sistema informático no conocen medidas de prevención que se deben usar sobre el software, para evitar infecciones por causa de virus informáticos[126].

**Consecuencia**

- Puede haber pérdida de información digital, daños en el hardware y/o software o mal funcionamiento y lentitud en el procesamiento de datos, debido a daños o ataques al sistema informático, ocasionado por software malicioso debido a falta de controles en el acceso a páginas no autorizadas de internet, esto se da por desconocimiento de los operarios de medidas de prevención y falta de software antivirus no instalados o actualizados

**Recomendaciones**

- Implementación de políticas de comunicaciones y navegación segura en Internet.

- La IPSI Guaitara, debe adquirir software de protección y actualización automática que detecten y eliminen amenazas de virus informáticos que pongan en riesgo el sistema informático.

- Los empleados, deben tener en cuenta aspectos básicos de seguridad informática, para evitar la infección por causa de virus informáticos del software y sistema informático de la institución.

[125] Hallazgos DS5(4)
[126] Hallazgos DS5(4)

# 4. CONCLUSIONES

- La auditoría de sistemas representa un gran factor de importancia para todo tipo de empresas, puesto que permite mayor control, seguridad y respaldo de la información procesada por los sistemas informáticos. La información es uno de los principales activos de las empresas, puesto que acumula un valor agregado que permite toma de decisiones oportunas, sin embargo está expuesta a riesgos físicos, lógicos o humanos, debido a vulnerabilidades que se contrarrestar con controles y recomendaciones dadas.

- Después de los resultados obtenidos, se logra evidenciar la importancia de identificar en cada organización vulnerabilidades y riesgos que afectan a los sistemas informáticos, brindando la oportunidad de identificar el estado del software de gestión y de esta manera evitar contratiempos para que no afecten el correcto funcionamiento de los procesos y se aumente la seguridad en base a la gestión de políticas de gestión de riesgos.

- Se puede inferir que la auditoría de sistemas permite la evaluación de normas y procedimientos que están establecidos en una empresa, esa evaluación busca la confiabilidad, seguridad y confidencialidad de la información para su análisis y la toma de decisiones por parte del área administrativa y gerencial.

- El proceso de auditoría permitió establecer que en la IPS Indígena Guaitara no existe documentación de políticas, procedimientos, seguridad y planes de contingencia que permitan el análisis y la gestión de procesos y riesgos para la identificación y clasificación de estos. La implementación de estas políticas, permitirán no solo reducir tiempos en capacitación de nuevos empleados, si no, también prestar un mejor servicio a la hora de presentarse inconvenientes.

- El modelo COBIT es utilizado como un marco de referencia para la dirección de Tecnologías de Información, puesto que permite evaluar características como efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, que permiten establecer hallazgos y recomendaciones para los dominios, logrando de esta manera la evidencia de oportunidades de mejoramiento en el procesamiento de la información.

- Con el desarrollo de este trabajo, la entidad tiene un insumo, para establecer controles y generar políticas de seguridad sobre su sistema informático, en especial sobre el software INFO-SALUD, con el objetivo de facilitar la toma de decisiones a nivel administrativo y gerencial para un funcionamiento más eficiente de los procesos que se utiliza en el aplicativo informático.

# 5. RECOMENDACIONES

- Iniciar un proceso de auditoría se hace fundamental para analizar todo el entorno organizacional, debido a que, como en todo sistema informático, cada componente se ve afectado si alguno de ellos presenta falla o ralentiza.

- Concientizar a las empresas, para promover la realización periódica de auditorías de sistemas, con el fin de fortalecer el proceso de manejo de información y adquisición de herramientas tecnológicas que agilice la eficiencia en los procesos, logrando así confiabilidad.

- Establecer la importancia que toda entidad tenga planes de contingencia en sus políticas organizacionales, para lograr continuidad de los servicios y así la empresa pueda lograr calidad, seguridad y eficiencia a la hora de realizar un proceso.

- Tener una política de capacitación orientada a los empleados sobre tecnologías de información y comunicación donde se pueda determinar que la tecnología no es un factor de retraso en los procesos, si no por el contrario es un aliado estratégico que permite agilidad y facilidad en procesos de gestión de datos e información.

- Entrenar y capacitar mantiene a los empleados enfocados y al día sobre las maneras más efectivas de hacer su trabajo, sin entrenamiento, los empleados tienen menos probabilidades de completar las tareas de forma eficaz y con eficiencia suficiente, esto puede causar ralentizar la prestación de los servicios de la institución y desmejorar la buena imagen de la institución. Una vez que la calidad en el servicio se reduce, se vuelve más difícil dedicar tiempo y dinero a la capacitación y al mantenimiento del software.

- Establecer en toda entidad documentación técnica sobre la instalación y operación del software, registro de funcionalidades o medidas en caso de errores, para que se logre resolver inconvenientes o dudas en el manejo de forma más efectiva, permitiendo así un funcionamiento más eficiente en la entidad.

- Evitar la dependencia de trabajadores, debido a que en caso de la dejación del cargo causa retrasos, puesto que los tiempos de adaptación del nuevo personal toma su tiempo.

## REFERENCIAS BIBLIOGRÁFICAS


- [1] Este trabajo en el desarrollo de la auditoría, 2015
- [2] SIGWEB, MatrizdeRiesgo, http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf [Consulta: 20 de Junio de 2015]
- [3] Material facilitado por la IPS Indígena Guaitara, 2014

## BIBLIOGRAFÍA


- ARENS, ALVIN A. Auditoría un Enfoque Integral, 6 Edición. México: Prentice Hall, 1996

- GUERRERO JAIRO, GOMEZ EDUARDO, TIMARAN RICARDO, CHAMORRO VICENTE, JARAMILLO NELSON, BOLAÑOS MANUEL, MARTINEZ DORIS, Guía para la elaboración de anteproyecto de grado, Universidad de Nariño, Mayo 2004

- MUÑOZ R, Carlos . Auditoría en sistemas computacionales. Mexico: Pearson Education, 2002.

- PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: Un enfoque práctico, 2° Ed., Alfa omega/RA-MA, Mexico,2001

- PINILLA F, José D. Auditoría Informática un enfoque operacional, ECOE, Bogotá, 1995.

## WEBGRAFÍA


- http://auditordesistemas.blogspot.com/
  Auditoría Informática y de Sistemas
  Solarte Francisco Nicolás
  Consultado el 20 de Octubre 2014

- http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf
  Seguridad en Informática (Auditoría de Sistemas)
  Álvarez Luis Miguel
  Consulta el 20 de Octubre de 2014

- http://aobauditores.com/funcion-auditor/

  «La Función del Auditor» (en español).

  Murillo, Enrique

  Consultado el 26 de marzo de 2014.

- http://es.wikipedia.org/wiki/Auditor
  Auditor
  Wikipedia Enciclopedia Libre
  Consultado el 20 de Agosto 2014

- http://www.mcgraw-hill.es/bcv/guide/capitulo/8448178971.pdf
  Auditoría: Concepto, clases y evolución
  Mheducation
  Consultado el 20 de Agosto de 2014

- http://dspace.ucuenca.edu.ec/bitstream/123456789/652/1/ts205.pdf
  Auditoría Informática- SUPERTEL
  Quintufa Karina Verónica
  Consultado el 21 de Agosto de 2014

- http://www.sindicom.gva.es/premi/files/auditoría%20sistemas%20inf_ok.pdf

- http://es.wikipedia.org/wiki/Sistema_de_salud_en_Colombia
  Wikipedia la enciclopedia libre
  Sistema de Salud en Colombia
  Consultado el 24 de Agosto de 2014

- http://www.minsalud.gov.co/Normatividad/LEY%201122%20DE%202007.pdf
  Ministerio de Salud
  Decreto Congreso de la república de Colombia
  Consultado el 6 de Septiembre de 2014

- http://www.supersalud.gov.co
  SUPERSALUD
  Veeduría Ciudadana
  Consultado el 9 de Diciembre de 2014

- https://www.invima.gov.co/index.php?option=com_content&view=article&id=806%3Alistado-codigo-unico-de-medicamentos&catid=213%3Aconsultas-registros-y-documentos-asociados&Itemid=428
  INVIMA
  Listado código único de medicamentos
  Consultado 8 de Marzo de 2015

- http://www.minsalud.gov.co/salud/Paginas/Normatividad-SISMED.aspx
  Ministerio de Salud
  Sistema de Medicamentos -SISMED de la Comisión Nacional de Precios de Medicamentos.
  Consultado 20 Abril de 2015.

- http://web.sispro.gov.co/WebPublico/SISMED/LibroVirtual/index2.html
  Ministerio de la Protección Social
  SISMED
  Consultado 20 Abril de 2015.

- https://www.minsalud.gov.co/Documentos%20y%20Publicaciones/Lineamientos%20T%C3%A9cnicos%20para%20EAPB%2009092013.pdf
  Ministerio de la Protección Social
  Lineamientos técnicos para el registro de los datos del registro individual de las prestaciones de salud-RIPS
  Consultado 5 de Mayo de 2015

# ANEXOS

## ANEXO A. ARCHIVO PERMANENTE

Información proporcionada por la IPS. Indígena Guaitara. Dicha información se encuentra en formato digital, organizada en un DVD tal como se indica a continuación.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO A. Archivo Permanente

Ahí adentro encontrara los siguientes archivos y carpeta.

- Portafolio de Servicios IPSI Guaitara.pdf
- Manual de Funciones.pdf
- Hoja de Vida Equipos de Computo.pdf
- Empleados_2015
    - Empleados_2015(1).jpg
    - Empleados_2015(2).jpg

## ANEXO B. DOMINIO PLANEACIÓN Y ORGANIZACIÓN

En este anexo es posible encontrar ordenado en tablas los cuadros de definición de fuentes de conocimiento que contienen las diferentes fuentes de información utilizadas para la evaluación de los criterios seleccionados, Cuestionarios utilizados, Hallazgos y Recomendaciones realizadas en el proceso de auditoría. Se encuentran en forma digital, organizados en un DVD tal como se indica a continuación.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO B. Dominio Planeación y Organización

## ANEXO C. CONTRATO SOFTWARE INFO-SALUD

Contiene documentación en donde se puede detallar el modelo, costo y características del contrato pactado, entre el proveedor y la I.P.S. Indígena Guaitara

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO C. Contrato Software Infosalud

Ahí adentro encontrara los siguientes archivos:

- Contrato_Soporte_Infosalud.docx
- Cuenta_Cobro_Ipiales_Guaitara.pdf
- Propuesta_Soporte_Ipiales_Guaitara.pdf

## ANEXO D. ENTREVISTAS_AUDIO

Contiene los audios de las diferentes entrevistas realizadas por el grupo auditor. Dichas entrevistas se encuentran en formato digital, organizadas en un DVD tal como se indica a continuación.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO D. Entrevistas_Audio

Ahí adentro encontrara los siguientes Archivos:

- Entrevista_Aux_Atencion_Usuario.mp3
- Entrevista_Aux_Facturacion.mp3
- Entrevista_Auxiliar_Higiene_Oral.mp3
- Entrevista_Coordinador_Facturacion.mp3
- Entrevista_DirectorAdministrativo.mp3
- Entrevista_DirectorServicioFarmaceutico.mp3
- Entrevista_HigienistaOral.mp3
- Entrevista_IngSistemas.mp3
- Entrevista2_IngSistemas.mp3
- Entrevista3_IngSistemas.mp3
- Entrevista4_IngSistemas.mp3
- Entrevista_MedicoAuditor.mp3
- Entrevista_MedicoGeneral.mp3
- Entrevista2_MedicoGeneral.mp3
- Entrevista_PersonalKardex.mp3
- Entrevista2_Aux_Atencion_Usuario.mp3

## ANEXO E. ENTREVISTAS_PREGUNTAS_ABIERTAS

Contiene las diferentes entrevistas abiertas realizadas por el grupo auditor. Dichas entrevistas se encuentran en formato digital, organizadas en un DVD tal como se indica a continuación.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO E. Entrevistas_Preguntas_Abiertas

Ahí adentro encontrara los siguientes Archivos:

- Entrevista_DirectorAdministrativo.jpg
- Entrevista1.jpg
- Entrevista2.jpg
- Entrevista3.jpg
- Entrevista4.jpg
- Entrevista5.jpg
- Entrevista6.jpg
- Entrevista7.jpg
- Entrevista8.jpg
- Entrevista9.jpg
- Entrevista10_Ingeniero.jpg
- Entrevista11_Ingeniero.jpg
- Formato Entrevista Abierta Ingeniero de Sistemas.docx

## ANEXO F. ENTREVISTAS_PREGUNTAS_CERRADAS

Contiene las diferentes entrevistas cerradas realizadas por el grupo auditor. Dichas entrevistas se encuentran en formato digital, organizadas en un DVD tal como se indica a continuación.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO F. Entrevistas_Preguntas_Cerradas

Ahí adentro encontrara los siguientes Archivos:

- Entrevista ingeniero(1).jpg
- Entrevista ingeniero(2).jpg
- Formato de entrevista Cerrada Ingeniero de Sistemas.docx
- Gráficos de Resultados Entrevistas Ipsi Guaitara.pdf

## ANEXO G. IMÁGENES DE PRUEBAS

Contiene las diferentes pruebas realizadas por el grupo auditor al software en donde se encontró oportunidades de mejoramiento. Dichas imágenes se encuentran en un archivo pdf formato digital con su respectiva imagen y descripción.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO G. Imágenes de Pruebas

Ahí adentro encontrara el siguiente Archivo:

- Imágenes de Pruebas Realizadas al Software INFO-SALUD.pdf

## ANEXO H. VIDEOS DE PRUEBAS

Contiene videos de pruebas realizadas por el grupo auditor al software en donde se encontró oportunidades de mejoramiento. Dichos videos se encuentran formato digital.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO H. Videos de pruebas

Ahí adentro encontrara los siguientes Archivos:

- Demostracion_accespv.mp4
- Instalacion_tesis_INFOSALUD.mp4
- Video_AuxOdontologia_Funcionamiento.mp4
- Video_Kardex_Funcionamiento.mp4
- Video_MedicinaGnrl_Funcionamiento.mp4
- Video_MedicoAuditor_Funcionamiento.mp4
- Video_Odontologia_Funcionamiento.mp4

## ANEXO I. VIDEOS DE GUÍA PROVEEDOR

Contiene los videos entregados por el proveedor que representan la única ayuda de soporte entregada por el proveedor. Los videos se encuentran en formato digital.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO I. Videos de Guía Proveedor

Ahí adentro encontrara los siguientes Archivos:

- Historia
  - Cirugias.mp4
- Instalacion
  - Instalacion.mp4
- Kardex
  - Entradas_01.mp4
  - Entradas_02.mp4
  - Tablas_Kardex.mp4
- Procesos
  - 001_Carga_Base_Aseguramiento.mp4
  - 002_Factracion_Demanda_Inducida.mp4
  - 003_Generacion_Reporte.mp4
  - 004_Generacion_Reporte.mp4
  - 005_Generacion_Reportes.mp4
  - 006_Perfil_Epidemiologico.mp4
  - 007_Archivos_Planos.mp4
  - 008_filtros1.mp4
  - 009_Migracion_Datos.mp4

## ANEXO J. INFORME EJECUTIVO

Contiene el informe ejecutivo entregado a las directivas de la IPS INDÍGENA GUAITARA en donde se detalla las oportunidades de mejoramiento en cada uno de los procesos evaluados por el grupo auditor.

Para acceder hay que ingresar a la carpeta:
Evidencias/ANEXO J. Informe Ejecutivo

Ahí adentro encontrara el siguiente archivo:

- Informe Ejecutivo de Auditoría.docx