AUDITORIA AL MODULO DE INVENTARIO DEL SISTEMA DE INFORMACION EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

DENIS ALFREDO COLUNGE BELALCAZAR
JORGE ALEXIS PORTILLA VARGAS

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

AUDITORIA AL MODULO DE INVENTARIO DEL SISTEMA DE INFORMACION EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

DENIS ALFREDO COLUNGE BELALCAZAR
JORGE ALEXIS PORTILLA VARGAS

Proyecto de Grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

ASESOR:
FRANCISCO NICOLAS SOLARTE SOLARTE
Mg. Maestría en Docencia

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

NOTA DE RESPONSABILIDAD

“Las ideas, recomendaciones y conclusiones planteadas en este trabajo de grado son de responsabilidad exclusiva de los autores”

Artículo 1 del acuerdo No. 324 de octubre 11 de 1966, emanado del 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 para su publicación priman las normas sobre el derecho de autor”

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

NOTA DE ACEPTACION

_____

_____

_____

_____

JURADO

_____

JURADO

San Juan de Pasto, 25 mayo de 2013

AGRADECIMIENTOS

En primer lugar a DIOS, que es el guiador de todo el universo. Y sin el auxilio del todo poderoso nada hubiere sido posible.

A la UNIVERSIDAD DE NARIÑO le expresamos nuestros agradecimientos, gracias por existir, gracias por ser una universidad pública a pesar de las adversidades y a su vez gracias por brindarnos la oportunidad de culminar nuestros estudios con éxitos.

Le agradecemos inmensamente a todo el personal del Hospital Universitario Departamental de Nariño, que ha puesto su grano de arena en el desarrollo de este trabajo de grado, en especial al ingeniero **Orlando García**.

A los ingenieros Francisco Solarte, Javier Villalba y Nelson Jaramillo, asesor y jurados de este proyecto, porque sin su colaboración y orientación en esta investigación hubiera sido muy difícil la culminación con éxitos de este proceso.

DEDICATORIA

Este éxito se lo dedico a mis padres, por su apoyo y esfuerzo absoluto, el cual fue de gran importancia en el transcurso de mi carrera.

A mis hermanos, en especial a Jhon Jairo Colunge Belalcázar, que aunque no fue posible verme cumplir con unos de mis objetivos más grandes, sé que está en el cielo derramándome lluvia de bendiciones.

A mis familiares y amigos que siempre estuvieron pendientes durante este lapso de tiempo en la Universidad, les agradezco con toda mi alma.

Denis Alfredo Colunge Belalcázar

RESUMEN

La auditoría al Sistema de Información del Hospital Universitario Departamental de Nariño en el módulo de inventario, se orientó fundamentalmente en hallar dificultades o falencias en las entradas y salidas de este, así como también seguridad física y lógica, lo cual permitió proponer recomendaciones pertinentes para cada hallazgo durante el proceso de auditoría. Para concluir con éxito este proyecto se tomó como marco de referencia el COBIT (objetivos de control para tecnologías de la información), en conjunto con los diferentes procesos de los pilares de este, planear y organizar, adquirir e implantar, entregar y dar soporte y monitorear y evaluar. Posteriormente se eligieron adecuadamente los procesos con sus respectivos objetivos de control de manera que estuvieran acorde con los objetivos de esta investigación. Aunado a lo anterior se elaboraron fuentes de conocimientos, cuestionarios cuantitativos, entrevistas, plan de pruebas y la matriz de probabilidad e impacto para calificar los diferentes hallazgos.

Una vez terminado el proceso de auditoría y teniendo en cuenta la misión y visión del Hospital Universitario Departamental de Nariño, se elaboraron unas conclusiones y recomendaciones respecto a la seguridad física y lógica y a su vez respecto a las entradas, trazabilidad y salidas de información del DGH.

ABSTRACT

Audit Information System Department, University Hospital of Nariño in the Inventory Module, is mainly focused on finding difficulties or shortcomings in the inputs and outputs of this, as well as physical and logical security, which allowed us to propose recommendations for each finding found during the audit process. To successfully complete this project is taken as the COBIT framework (Control Objectives for Information Technology), in conjunction with the different processes of the pillars of this, plan and organize, acquire and implement, deliver and support and monitor and evaluate. Subsequently chose processes adequately control their goals so that they were consistent with the objectives of this research. Added to this were developed knowledge sources, quantitative questionnaires, interviews, test plan and probability and impact matrix to describe the different findings.

Once the audit process, taking into accounts the mission and vision of the University Hospital Department of Nariño, conclusions were drawn and recommendations for physical and logical security and in turn respect to the inputs and outputs trace information DGH.

TABLA DE CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO FIJO: se considera activo fijo a todo bien de la empresa que es destinado para su beneficio. Es decir es aquel que es explotado por la institución.

ACTIVO MÓVIL: se considera activo móvil aquel bien que es destinado a la comercialización.

ÁREAS: áreas se refiere a cada una de las dependencias de la organización.

BENEFICIO: se considera como beneficio a la utilidad o la compensación moral o material obtenida por una inversión.

BODEGA: bodega es el espacio de alojamiento de los activos tanto fijos con variables de una organización.

CONTRASEÑA: contraseña se refiere al conjunto de caracteres que le permiten el acceso a un usuario a utilizar cierta proporción de un sistema o a una red.

COSTOS: se considera como costo al valor obtenido en la producción de un determinado producto. El cual permite el precio de venta de un de dicho producto.

ELEMENTOS PERECEDEROS: Estos hacen referencias aquellos activos que caducan con el tiempo.

FARMACIA: farmacia es el lugar donde se expiden todos los productos relacionados con salud, en especial medicamentos.

GRUPO: grupo se refiere a un conjunto de provisiones, los cuales están escritos en una tabla con su código y nombre.

INFORME: informe se refiere a cada uno de los documentos generados por el sistema. Los cuales coadyuvan en la toma de decisiones.

INVENTARIO: un inventario es un conjunto de activos tanto fijos como móviles con lo cual cuenta la organización para su beneficio o comercialización.

IVA: este hace referencia al impuesto de valor agregado por cada producto en una organización.

MÓDULOS: módulos hace referencia a cada uno de las grandes divisiones de un programa de aplicación.

MOVIMIENTOS DE PRODUCTOS: hace referencia al registro de la vasta gama de productos que se registran en un sistema.

PRODUCTOS: producto se define como el resultado de un proceso, ya sea mecánico o industrial. Con el objeto de ser ofrecido en un mercado.

PRODUCTOS DEPRECIABLES: estos hacen referencias aquellos activos que disminuyen su valor con respecto al tiempo.

PROVEEDORES: se consideran como proveedores a todos aquellos que abastecen a la institución, de bienes y servicios.

REGISTRO: registro hace referencia a un conjunto de campos que se asientan en un sistema, que en conjunto proporciona información.

SOFTWARE: software se refiere al conjunto de programas que son utilizados en computación para diversos fines.

SUBGRUPO: subgrupo hace referencia a una subclase de un grupo, es decir que estos están dentro de los grupos con lujos y detalles.

TIPOS DE CONTRATO: hace referencia al documento que especifica el acuerdo entre el empresario y la institución.

TRAZABILIDAD: es el camino o recorrido que sigue la información o los productos desde el inicio hasta el fin, en un área de una organización con respecto a la interacción con otras áreas.

UNIDADES DE MEDIDA: hace referencia al patrón de medida (moneda) estándar que se ocupa para la obtención de bienes y servicios.

USUARIO: usuario se refiere a la persona que hace uso de los recursos de cómputo que le son suministrados por el administrador del sistema o la red.

VENCIMIENTO DE PRODUCTOS: es la caducidad legal de un determinado producto, la cual fue previamente otorgada por el fabricante.

VENTAS: ventas se refiere al ejercicio de traspaso de un producto a un cliente, efectuándose de manera legal es decir previamente documentada.

INTRODUCCIÓN

En la actualidad el HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO cuenta con un Sistema de Información, DINAMICA GERENCIAL HOSPITALARIA (**DGH**), que se encarga de manejar toda la información hospitalaria en dos grupos de módulos los cuales funcionan de forma interdependiente; primero son los módulos financieros que se encargan de administrar la información para realizar los procesos de previsión, planeación, organización, integración, dirección y control, para poder manejar los recursos económicos de la forma más óptima posible. Segundo son los módulos de médico-asistencial que se encarga de administrar la información para realizar las funciones de organizar, coordinar, dirigir, supervisar y evaluar las ejecuciones de todas las acciones de salud del hospital, a este grupo pertenece el módulo de inventario al cual se le efectuó la auditoria.

Un inventario es el registro total de los bienes y demás cosas pertenecientes a una persona o comunidad, hecho con orden y precisión. Por extensión, se denomina inventario a la comprobación y recuento, de las existencias físicas en sí mismas y/o con las teóricas documentadas. El módulo de inventario del (SIGH) permite administrar y crear los medicamentos así como los insumos manejados por el Hospital Universitario Departamental de Nariño.

Esta auditoría consistió en evaluar el módulo de inventario, tomando como punto de referencia el COBIT (*Control objectives for information and related technology*), ya que este proporciona los parámetros que hay que tener en cuenta para llevar a cabo esta auditoría.

Por otro lado esta auditoria se elaboró en cuatro etapas que son : fase de conocimiento la cual implicó todo el proceso de recolección de la información, fase de análisis y evaluación de riesgos la cual radicó en identificar los riesgos, vulnerabilidades y amenazas halladas durante el proceso, fase de ejecución de pruebas esta se refiere a la clara elaboración de un plan de pruebas y que luego fueron ejecutas con mucho rigor, y cuarta y última, la fase de presentación de hallazgos consistió en elaborar un informe claro y conciso de las anomalías encontradas durante la experiencia.

Esta auditoría se realizó con el objetivo de verificar el estado del módulo de inventario, la cual permitirá mejorar la trazabilidad de la información hospitalaria, además de un eficaz y eficiente tratamiento a todos los recursos hospitalarios, bajo normas y estándares de calidad. Aunado a lo anterior, esta auditoría evaluó la calidad en cuanto a la eficacia y eficiencia del funcionamiento del módulo de inventario, para comprobar el momento de este. Y de esta manera, poder determinar la confiabilidad de las entradas y las salidas relacionadas con el módulo de inventario. Posteriormente con los resultados adquiridos se recomendaron estrategias de mejoramiento a este módulo, para optimizar los servicios prestados por el Sistema de Información del Hospital Universitario Departamental de Nariño.

1. ALCANCE Y DELIMITACIÓN

La información es el activo más importante dentro de cualquier organización. Cada vez existe un mayor requerimiento de información fidedigna en el entorno hospitalario, que se presenta de varios tipos como es la información externa, interna, administrativa y de gestión. Esta es manejada en el módulo de inventario del sistema de información integrado del Hospital Universitario de Nariño, El cual le permite controlar los ingresos y salidas de mercancías por cualquier concepto, además permite establecer estadísticas, costos, rentabilidad y movimientos de cada uno de los productos. En el transcurso de la auditoria se encamino a evaluar las entradas y las salidas correspondientes al módulo de Inventario, que permiten controlar los medicamentos así como los insumos manejados por el hospital, inspeccionando de forma eficaz y eficiente la administración de insumos y medicinas. Este módulo posee interfaces directas con los módulos de Facturación y Presupuesto. Durante el transcurso de la auditoria se realizó la evaluación de las entradas y las salidas al Módulo de Inventario junto con las interfaces que este tiene relación, es decir se verificó la trazabilidad de todos y cada uno de los movimientos que este Módulo maneja.

Las entradas al módulo de inventario del DGH del HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO, son:

Orden de Compra
Remisión de Entrada
Comprobante de entrada
Devolución de Ventas
Devolución de Suministro
Solicitudes

Las salidas del módulo de inventario del DGH del HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO, son:

Suministro de Paciente
Remisión de Salida
Pedido y Factura
Devolución de Compras
Solicitud de pedido

1.1 FACTIBILIDAD DE LA INVESTIGACIÓN

Para el desarrollo de la auditoria al módulo de inventario del Sistemas de Información del Hospital Universitario Departamental de Nariño, se tienen los recursos necesarios y los medios con respecto a aspectos como: presupuesto, recurso humano y todo con lo que tiene que ver con hardware y software.

1.1.1 Factibilidad técnica. Para el desarrollo de la auditoria al módulo de inventario del Sistemas de Información del Hospital Universitario Departamental de Nariño, se contó con el (**DGH**) Dinámica Gerencial Hospitalaria que es el software actual que se ejecuta en el Hospital, diccionario de datos, grabadoras, impresoras, cámaras fotográficas y computadores.

1.1.2 Factibilidad operativa. Tanto el departamento de sistemas como el personal administrativo del Hospital Universitario Departamental de Nariño son conscientes de que esta auditoría ayudará de manera reveladora a tomar las decisiones del control adecuado, sobre la administración del módulo de inventario.

1.1.3 Factibilidad económica. El actual proyecto de auditoría figurará en un documento, que tanto en el área de sistemas como en áreas administrativas y demás podrán utilizar de tal manera que, tomen decisiones oportunas que coadyuven a lograr un excelente servicio prestado por el hospital, ya que si mejoramos el manejo del software, mejoran los servicios a los usuarios y a su vez a la organización.

El proyecto no presentó gastos elevados, por lo cual se financió por el grupo investigador.

2. MARCO REFERENCIAL

2.1 MARCO CONTEXTUAL

2.1.1 Información general y ubicación del HUDN. El Hospital Universitario Departamental de Nariño es una empresa social del estado, ubicado en la ciudad de San Juan de Pasto del departamento de Nariño (Colombia) sus datos son los siguientes:

- Dirección: Calle 22 No 7-93 Parque Bolívar.
- Teléfono: 7214525 – 7214526
- Fax: 7214530
- Web: www.hosdenar.gov.co

El Hospital Universitario Departamental de Nariño, acoge plenamente las directrices de la alianza mundial para la seguridad del paciente que promueve a la organización mundial de la salud, en este marco la organización promoverá la ejecución de estrategias en cinco áreas con la finalidad de reducir efectivamente la ocurrencia de eventos adversos.

- De la organización
- De la formación y la cultura
- De la evaluación
- De los sistemas de información y comunicación
- De la investigación

En la actualidad el Hospital Universitario Departamental de Nariño cuenta con un sistema de información compuesto por dos grandes subsistemas, los cuales son:

Administrativo:

- Pagos
- Contabilidad
- Inventarios Hospitalarios
- Nomina
- Facturación
- Cartera
- Presupuesto
- Costos Hospitalarios
- Tesorería
- Activos fijos

Asistenciales:

- Admisiones
- Hospitalización de citas Medicas
- Consulta Externa
- Contratos
- Administrativos de recursos
- Historia clínica electrónica

2.1.1.1 Misión. El Hospital Universitario Departamental de Nariño, es una empresa social del estado, con vocación académica, que complementa con altos estándares de seguridad a la red departamental de prestadores de servicios de salud en mediana y alta complejidad. Además respalda el crecimiento de talento humano, lo cual permite proyectarse e incidir en el mejoramiento de la salud y calidad de vida de la comunidad del sur occidente colombiano[1].

2.1.1.2 Visión. El Hospital Universitario Departamental de Nariño E.S.E, enfocará todos sus esfuerzos al mejoramiento continuo, se convertirá en una institución centrada en el usuario, aunado a esto fortalecerá la implementación de tecnología, de manera que se complemente la red de prestadores de servicios de salud del Departamento de Nariño[2].

2.1.1.3 Objetivos estratégicos

- "Mantener el Sistemas Único de Acreditación SUA: seguridad del paciente, atención más humana, disminución del riesgo y tecnología al servicio de la vida.

- Gestionar la implementación del Sistema Integral HSEQ: Calidad (ISO 9001) Gestión Ambiental (ISO 140001), Seguridad Industrial y Salud Ocupacional. (ISO 18001).
- Conservar un bajo nivel de riesgos financiero y jurídico, mediante una administración eficiente y efectiva de los recursos.

- Mejorar la capacidad instalada (ampliar la infraestructura física adquisición de nueva tecnología y dotación institucional hospitalaria).

[1] Archivo [pdf] PLAN DE DESARROLLO, HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.-Adobe Reader.p.83.

[2] Ibíd., p.84.

- Mejorar el desarrollo integral del talento humano, con énfasis en los programas de humanización del servicio.

- Ampliar el portafolio de servicios orientados a Supra-Especialidades.

- Fortalecer los Convenios Docencia-Servicios y la Investigación Científica"[3].

2.1.2 Servicios hospitalarios[4]

A. Servicios ambulatorios

El Hospital Universitario Departamental de Nariño E.S.E dispone de la oferta de servicios médicos más amplia del Departamento y es centro de referencia en las diferentes especialidades.

Consulta externa

Esta área consta de 24 consultorios cómodamente dotados, con la tecnología necesaria para la atención segura de los pacientes, zonas comunes, sala de espera, oficinas de atención al usuario y ascensor para personas discapacitadas. La atención es prestada por 60 médicos especialistas, una enfermera y 12 auxiliares de enfermería.

Especialidades clínicas

- Anestesiología
- Cardiología
- Endocrinología
- Gastroenterología
- Hematología
- Medicina Interna
- Neurología Clínica
- Oncología
- Fisiatría
- Dermatología
- Ortopedia

[3] Ibíd., p.84.

[4] Archivo [pdf] PORTAFOLIO DE SERVICIOS, HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.-Adobe Reader.P.11-27.

- Oftalmología
- Otorrinolaringología
- Ginecología
- Urología
- Cirugía General
- Cirugía Plástica
- Neurocirugía
- Nutrición

Procedimientos de pequeña cirugía

- Cirugía Plástica
- Dermatología

Procedimientos médicos

- Gastroscopia
- Colonoscopia
- Rectosigmoidoscopia
- Enteroscopia
- Cistoscopia

Exámenes diagnósticos

- Electrocardiograma
- Electroencefalograma

Atención al usuario

En el área de consulta externa se encuentra el servicio de atención al usuario, bajo la dirección de profesionales de trabajo social que se encargan de orientar al paciente y su familia sobre los tramites de ingreso y egreso del hospital, requisitos para la atención, orientación sobre derechos y deberes, e inquietudes sobre la seguridad social. Además, se presta atención al paciente y su familia en situaciones como:

- Enfermedades crónicas
- Rehabilitación
- Fase terminal de una enfermedad

B. Servicios hospitalarios

Urgencias

Este servicio trabaja de manera integral las urgencias de adultos las 24 horas del día, 365 días al año, con disponibilidad permanente del personal en todas las especialidades básicas y de alta complejidad.

Se cuenta con:

- Atención de urgencias por médicos generales
- Atención de urgencias por médicos especialistas
- Atención por otros profesionales de la salud
- Apoyo diagnostico
- Soporte terapéutico

Estancias de observación

Servicios de hospitalización

Este servicio es prestado a usuarios que requieren atención integral por problemas de salud y que necesitan de vigilancia profesional permanente, para su diagnóstico, recuperación y/o tratamiento. Posee ambientes confortables y seguros para los pacientes y sus familiares.

Habitaciones y suites

En este servicio se encuentran disponibles cómodas habitaciones unipersonales y suites dotadas de tecnología para la atención integral de los pacientes, con baño privado, televisión, internet, sala, cajas de seguridad y sofá cama para acompañantes, brindando mayor confort para una estancia más agradable tanto del paciente como de sus acompañantes.

Unidad de cuidados intensivos

El Hospital Universitario Departamental de Nariño cuenta con una unidad de cuidados intensivos de adultos. Su equipo lo conforman médicos internistas con formación en cuidado intensivo. Se presta un servicio de alta calidad técnica y humana a los pacientes en estado crítico y a sus familias, durante las 24 horas del día, los 7 días de la semana.

Triage

Hace parte del servicio de urgencias, aquí el paciente es evaluado por médicos generales, encargados de priorizar la atención de acuerdo a su estado, con el fin de brindar mayor seguridad, proteger la vida y disminuir el riesgo de las personas que ingresan.

C. Servicios de apoyo diagnóstico

Imagenología

En el área de imagenologia se realizan todos los exámenes diagnósticos simples y de alta complejidad con equipos de última tecnología y un grupo humano especializado, para prestar un servicio de excelente calidad, en beneficio de los usuarios.

Tomografía Axial computarizada de 64 detectores

El Hospital posee el más moderno equipo de Tomografía Axial Computarizada, el modelo Aquilón 64 de Toshiba que ofrece imágenes con la más alta resolución isotrópica y la menor dosis de radiación existente en el mercado. Permite realizar estudios de rutina, TAC helicoidal, reconstrucción tridimensional y multiplanar, TAC trifásico, estudio de nódulo pulmonar y estudios diagnósticos en cabeza y cuerpo, biopsias y drenajes, procedimientos intervencionistas, estudios especiales del tracto gastrointestinal y genitourinario.

Apoyo diagnóstico

Resonancia nuclear magnética

Este magneto superconductivo, permite realizar estudios diagnósticos en menos de 20 minutos, entre ellos:

- Estudios neurológicos: cerebro, columna, oídos, hipófisis, orbitas, hipocampo, perfusión cerebral.
- Estudios osteo articulares: rodilla, tobillo, pie, cadera, hombro, brazos, piernas, muñeca, codo, mano, coxofemoral, ATM.
- Estudios corporales: pelvis, abdomen, colangioresonancia, tórax, cuello, uroresonancia.

- Estudios vasculares: Angio cerebral, carótidas, aorta torácica, aorta abdominal, miembros inferiores, extremidades, espectroscopia cerebral.

Ecocardiografía

Se cuenta con un sistema de diagnóstico por ultrasonido, que ofrece excelente calidad de imagen, visualizando con absoluta precisión el más pequeño detalle tisular o estructura vascular, asegurando un mejor diagnóstico del sistema cardiovascular.

Clases de ecografía:

- Convencional
- Intraoperatoria
- Intracavitaria (transvaginal, transrectal)
- Doppler color
- Biopsias y drenajes
- Mamaria

D. Soporte terapéutico

Banco de sangre

Este servicio se encuentra habilitado por el INVIMA como Banco de categoría A, cuenta con equipos de última generación para el montaje de pruebas de Inmunohematología y la más avanzada tecnología para el procesamiento de sangre y producción de hemoderivados dentro de los cuales se encuentran: glóbulos rojos desleucocitados, plaquetas y plasma fresco congelado. Estos productos están siempre disponibles para el apoyo terapéutico de los pacientes.

Servicio farmacéutico

En esta área se realiza el suministro de medicamentos y dispositivos médicos, brindando al usuario y personal asistencial toda la información necesaria para su uso adecuado, logrando el cumplimiento de la farmacoterapia prescrita por el médico tratante y previniendo factores de riesgos derivados de su uso. La central de mezclas parenterales, cumple con altos estándares de calidad y seguridad, que garantizan la correcta preparación de medicamentos oncológicos, dosis unitarias de antibióticos y nutrientes parenterales.

Soporte nutricional

El soporte nutricional se brinda como parte del manejo integral al paciente hospitalizando, fundamental en la recuperación, disminución de las complicaciones y del tiempo de estancia. Las instalaciones cumplen con todos los estándares de higiene y manipulación de alimentos que incrementan la seguridad de los usuarios.

E. Servicios quirúrgicos

Se prestan los servicios de cirugía ambulatoria y hospitalaria en las diferentes especialidades, cuentan con quirófanos integrales equipados con tecnología que permite realizar procedimientos quirúrgicos de alta complejidad, sala de recuperación para los pacientes después de cirugía con camas monitorizadas y atención permanente de los médicos anestesiólogos y enfermeras.

- Especialidades Quirúrgicas
- Cirugía General Hospitalaria y Ambulatoria
- Traumatología y Ortopedia
- Cirugía Pediátrica
- Cirugía Plástica
- Ginecología y Obstetricia
- Neurocirugía
- Oftalmología
- Otorrinolaringología
- Urología
- Cirugía Dermatológica
- Cirugía Laparoscópica

F. Servicios ginecológicos y obstétricos

Sala de partos y hospitalización ginecobstétrica

En este servicio nuestras pacientes embarazadas pueden contar con atención especializada tanto en su parto normal como cuando presentan alguna complicación o patología ginecológica u obstétrica durante las 24 horas del día, con disponibilidad de salas de cirugía, unidades de cuidado intensivo y ayudas diagnósticas. Las madres gestantes son atendidas en salas para trabajo de parto y recuperación, construidas bajo los más altos estándares de calidad internacionales, ofreciendo mayor seguridad clínica a la madre y su hijo.

El área de ginecobstetricia cuenta con habitaciones unipersonales, y bipersonales cómodamente dotadas para hacer más agradable la estancia.

Neonatología

Esta área se encarga del manejo y tratamiento de las enfermedades médicas o quirúrgicas en la etapa de la vida de los 0 a los 28 días; aquí se establecen los cuidados mínimos, intermedios o intensivos según sean requeridos de acuerdo al estado crítico del recién nacido.

El hospital cuenta con el programas ampliado de inmunización al recién nacido, Vacunas: B.C.G, Hepatitis B, Triple Viral, Vacunación a mujeres en post-parto y post-legrado. Estimulación adecuada y tamizaje de TSH.

G. Servicios de rehabilitación y medicina física

El servicio de Medicina Física y Rehabilitación utiliza un conjunto de procedimientos elementos físicos con fines diagnósticos, terapéuticos y preventivos para mejorar el estado funcional de los pacientes, reintegrándolos a las actividades cotidianas, sus instalaciones están equipadas con sala de hidroterapia y la mejor tecnología disponible para rehabilitación física, respiratoria, ocupacional, del lenguaje. En esta área funciona además el Centro de Atención Integral a Víctimas de minas antipersona.

Ofrecemos servicios de:

- Fisiatría
- Terapia Respiratoria
- Terapia del Lenguaje
- Terapia Ocupacional

H. Servicios especiales

Unidad de oncología y radioterapia

A través de esta unidad se busca mejorar la prevención y cura del cáncer, brindando apoyo emocional, social y psicológico al paciente y su familia. Las nuevas instalaciones ofrecen a los pacientes, familiares y a los profesionales que los atienden unos espacios modernos, perfectamente equipados, adecuados a sus necesidades.

Planificación computarizada de los tratamientos de radioterapia

El hospital posee un moderno sistema que permite la planificación del tratamiento de radioterapia a través de simulación virtual en 3D, con un tomógrafo axial computarizado, mesa plan en fibra de carbono, láseres LAP “Dorado CT-4-3 red” y el sistema de planificación del tratamiento eclipse 8.0 uno de los mejores a nivel mundial, de esta forma de delimitan con gran precisión las áreas anatómicas, estableciendo un plan completo y específico para cada paciente.

Donde se ofrece servicios de:

- Quimioterapia
- Consulta de Oncología Clínica
- Sala de Quimioterapia
- Odontología
- Odontología Oncológica
- Soporte Oncológico
- Psicoterapia Individual y Grupal
- Asesoría Familiar

Otros de los servicios

- Atención integral a víctimas de minas antipersona
- Salud ocupacional
- Asesoría en planificación familiar
- Vigilancia epidemiológica y de salud publica
- Asesoría en lactancia materna
- Programa madre canguro
- Albergue a usuarios de escasos recursos “Una Esperanza de Vida”

I. Servicios logísticos y de apoyo

- Traslado Asistencial Básico
- Traslado Asistencial Medicalizado
- Nutrición
- Esterilización
- Vigilancia y Central de Monitoreo
- Facturación
- Central de Autorizaciones
- Call Center
- Auditorios con ayudas Virtuales
- Capilla

- Suministros y Almacén
- Cafetería
- Lavandería
- Morgue
- Gestión Ambiental
- Gestión de Emergencias y Desastres
- Mantenimiento equipamiento Biomédico e Infraestructura
- Servicios Generales
- Archivo central de correspondencia y de historias clínicas
- Central de gases medicinales
- Central electrógena
- Servicios administrativos en manejo y control de recursos financieros, recursos humanos, recursos físicos, recursos de sistema de gestión y de información.
- Asesoría y referenciación en: Auditoría Médica, Control Interno Disciplinario, Planeación, Calidad, Jurídica y Gestión Comunicacional.

2.1.3 Competencia. El Hospital Universitario Departamental de Nariño E.S.E y sus estamentos posee competencias en el departamento de Nariño, por ser catalogada como una entidad prestadora de servicios de salud del tercer nivel de complejidad.

2.2 MARCO LEGAL

El marco legal de la auditoria al módulo de inventario del Sistema de Información del Hospital Universitario Departamental de Nariño esta soportado por:

CONTRATO DE PRESTACIÓN DE SERVICIOS OJ 013- 2012 PARA ACTUALIZACION, MANTENIMIENTO y SOPORTE ENTRE EL HOSPITAL UNIVERSISTARIO DEPARTAMENTAL DE NARIÑO E.S.E y SISTEMAS Y ASESORIAS DE COLOMBIA S.A. El cual se anexa al documento final de este proyecto.

2.2.1 Ley 100 sistemas de información. Este marco legal no estaría íntegramente realizado si antes no se cierra con la ley que rige a todas las instituciones prestadoras de salud en COLOMBIA (ley 100 de 1993). El marco legal muestra el contexto institucional a nivel gubernamental en el cual se desarrollan los sistemas de información de la salud en Colombia. La Ley 100 de 1993, que reformó al sector salud en el país, en el objeto, fundamentos y características del sistema establece, entre otros:

Protección integral: El Sistema General de seguridad Social en Salud brindará atención en salud integral a la población en sus fases de educación, información y fomento de la salud y la prevención, diagnóstico, tratamiento y rehabilitación en cantidad, oportunidad, calidad y eficiencia, de conformidad con lo previsto en el artículo 162 respecto del Plan Obligatorio de Salud (6).

Desde el año de 1993, está establecida la función de informar como fundamental para el funcionamiento del sistema, sin embargo, la Ley 100 va más allá y define a responsabilidad de cada uno de los actores en cuanto a la información, especialmente la del Gobierno (Nacional y regional) de generar y difundir información relacionada con la salud, que incluya el estado de salud de la población, así como indicadores de precios, gestión y calidad.

Otros decretos y resoluciones reglamentan la conformación y contenidos de componentes del sistema, como el Sistema Obligatorio de Garantía de la Calidad (Resolución 1446 de 2006, Decreto 1011 de 2006) o el Sistema de Vigilancia (Decreto 1562 de 1984, Decreto 3518 de 2006), etc. El Plan de Desarrollo 2006-2010 (Ley 1151 de 2007) en la descripción de los principales programas de inversión establece la formulación de un Plan Nacional de Tecnologías de la Información y la Comunicación (TIC), para promover el aprovechamiento de las tecnologías, “el desarrollo de las infraestructura necesaria y los mecanismos de apropiación de la misma” (7). A raíz de este mandato incluido en el Plan de Desarrollo, el Ministerio de TIC ha venido liderando, con el apoyo de la academia y otras organizaciones, la implementación de programas de desarrollo de tecnologías de información dentro de las entidades gubernamentales. El Plan Nacional de TIC tiene como meta “en el 2019 todos los colombianos estarán conectados e informados, haciendo un uso eficiente y productivo de las TIC” (8). El plan contempla a la educación, salud, justicia y empleo como los ejes de desarrollo. En el tema de salud plantea como objetivo “lograr altos niveles de calidad y cubrimiento de los servicios de salud, a partir de la instalación de infraestructura tecnológica y la apropiación y uso eficaz de las TIC en el sector” (8). Los ejes de desarrollo en salud para el cumplimiento de éste objetivo son el Sistema Integrado de la Protección Social (Sispro) y el desarrollo de programas de telemedicina. En el informe del Consejo Privado de Competitividad en 2010, se refieren como estrategias para fortalecer la institucionalidad y masificación de las estrategias de TIC, entre otras:

- Fortalecer la institucionalidad del Plan Nacional de TIC y asegurar sus recursos estableciendo compromisos por parte de las entidades en el Plan Nacional de Desarrollo 2010-2014.
- Aumentar la asignación de recursos para programas de masificación de acceso y uso de TIC, así como facilitar su asequibilidad vía reducción de costos.

En salud, específicamente:

1. Digitalizar la totalidad de las historias clínicas y desarrollar una plataforma electrónica para facilitar su acceso en línea.

2. Identificar las zonas remotas con mayores niveles de morbilidad y mortalidad en el país para asegurar la presencia de telemedicina (8). Estas estrategias surgen de la necesidad de mejoramiento en la prestación de servicios y reducción de costos derivados de la facilidad de acceso a la información por parte de los profesionales de la salud y los ciudadanos. La Ley 1438 de 2011(4) busca reformar el Sistema General de Seguridad Social en Salud (SGSSS). En cuanto a información, establece la responsabilidad del Ministerio de Protección Social en el establecimiento de indicadores de desempeño para todos los actores y el desarrollo de un sistema de evaluación y calificación de cada uno de éstos que permita conocer de forma pública los resultados. Adicionalmente, establece que el Sispro debe estar integrado por los sistemas del Ministerio de Protección Social, Registraduría Nacional del Estado Civil, Ministerio de Hacienda y Crédito Público, Dirección de Aduanas e Impuestos Nacionales, el Sisben y las EPS.

Por otro lado, esta ley define la obligatoriedad de la digitalización de todas las historias clínicas a partir de diciembre de 2013. La conectividad de las instituciones vinculadas con el sector salud debe garantizarse antes de tres años de entrada en vigencia de la ley. El reporte de información es obligatorio para todos los actores del sistema, quienes están sujetos a sanciones en caso de incumplimiento. En cuanto a salud pública, se crea el Observatorio Nacional de Salud, a cargo del Instituto Nacional de salud, encargado de hacer el “monitoreo de los indicadores de salud pública, evaluaciones periódicos y formulación de recomendaciones”. Para la optimización de los procesos de priorización de los contenidos del plan de beneficios, crea un instituto de evaluación de tecnologías, dependiente del Ministerio de la Protección Social.

El desarrollo del sistema de información de la salud está soportado no sólo por la definición de roles en las leyes pertinentes, sino también por un plan nacional de fomento de la utilización de tecnologías de la información. A pesar de la presencia

de un marco legal, el Estado no ha tenido la fortaleza institucional para garantizar el cumplimiento de lo contenido en las normas.

La reglamentación, implementación y seguimiento es responsabilidad de los entes rectores del sistema, quienes deben tener los recursos y alcance suficiente para hacer entrar la normatividad en vigor.

3. Componentes del sistema de información en salud

El sector de la salud en Colombia cuenta con varios sistemas de información, los cuales frecuentemente no se encuentran integrados; esta situación ha llevado a una duplicación de esfuerzos para la generación de los reportes, y por tanto, a la baja calidad de la información recogida.

Como en la mayoría de sistemas de salud, se encuentran dos grandes grupos de actores: por un lado están los sistemas de información de los organismos públicos y por el otro los pertenecientes a instituciones privadas (prestadores de servicios de salud y agremiaciones, entre otras). Aunque las instituciones privadas también deben reportar a los sistemas de información gubernamentales, sus sistemas son independientes, no se encuentran integrados y no necesariamente son compatibles con los estatales. Incluso los prestadores de servicios públicos tienen en algunas ocasiones sus propios sistemas de información, que tampoco están integrados a los del Gobierno Nacional.

El Sistema de Vigilancia en Salud Pública (Sivigila) es un sistema de reporte de eventos de interés en salud pública, gestionado por el Instituto Nacional de Salud, que reporta especialmente patologías infecciosas, aunque recientemente se ha adicionado un módulo de mortalidad materna.

El Ministerio de la Protección Social, también cuenta con el Centro Nacional de Enlace, el cual utiliza principalmente la información producida por el Sivigila para reportar amenazas a la salud pública a organizaciones internacionales (9).

La estrategia gubernamental en torno a las TIC en salud se centra en la implementación de telemedicina y del Sispro (8). Esta bodega de datos es gestionada por el Ministerio de la Protección Social e integra la información de salud, pensiones, riesgos profesionales, trabajo, empleo y asistencia social. Cada fuente de información del Sispro tiene una estructura de reporte y consolidación independiente; los componentes del sistema son (3):

• **Registro Único de Afiliados (Ruaf):** maneja información de afiliación a todos los componentes de la protección social (salud, pensiones, riesgos profesionales, etc.). La información es reportada directamente por las administradoras al Ruaf, excepto salud que tiene un mecanismo de reporte diferente a través del Fondo de Solidaridad y Garantía (Fosyga). El Ruaf tiene un módulo llamado ND-Ruaf que registra la información de nacidos vivos y defunciones; este módulo es la fuente de información utilizada por el Departamento Nacional de Estadística (DANE) para la publicación de información poblacional.

• **Planilla Integrada de Liquidación de Aportes (PILA):** la PILA es la base de datos que maneja información de empleo, cotizantes y aportantes a los diferentes módulos de la protección social.

• **Sistema de Información de Precios de Medicamentos (Sismed):** el sistema de información de precios medicamentos registra datos de precios de compra y venta de medicamentos por parte de IPS, EPS, droguerías, etc.

• **Cuentas maestras:** contiene información de la distribución de recursos del sistema general de participaciones.

• **Registro de personas con discapacidad:** en esta base de datos se encuentran registradas personas con algún tipo de discapacidad que son reportadas por las gobernaciones. Esta base de datos tiene una baja cobertura, dada la dificultad para la identificación y el registro de ésta población.

• **Registro Individual de Prestación de Servicios (RIPS):** recoge la información de los servicios de salud prestados en el país. Estos registros son generados por las IPS, las cuales los envían a la administradora correspondiente, la que a su vez los envía al Ministerio de Protección Social.

En años anteriores han tenido algunos problemas de calidad y cobertura; sin embargo, desde 2009 se ha venido realizando un trabajo con las administradoras de planes de beneficios para mejorar la calidad y la cantidad de reportes.

Vacunación: contiene información de vacunación enviada por las direcciones territoriales de salud. Hacia el futuro este módulo se plantea como un sistema de seguimiento para cada individuo vacunado, con el objeto de supervisar el cumplimiento de planes de vacunación.

• **Sistema de Gestión de Hospitales Públicos (SIHO):** recoge información de gestión, capacidad instalada y funcionamiento de los hospitales públicos. No tiene alta cobertura.

• **Registro Especial de Prestadores de Servicios (REPS):** registra la información de los prestadores habilitados para la prestación de servicio. Es responsabilidad de los entes territoriales.

Los resultados del desarrollo del Sispro en general han sido positivos. El Gobierno Nacional tenía una meta para 2010 de 85% de la población validada o certificada en el sistema. Al 30 de septiembre de dicho año, el porcentaje reportado era del 87% de la población del país. Otro objetivo era contar con por lo menos el 65% de los programas sociales registrados en el Ruaf y el 45% de las fuentes del Sispro en la bodega de datos. Los valores de estos indicadores para septiembre de 2010 fueron de 57 y 113% respectivamente. En cuanto al porcentaje de entidades del orden nacional que ofrecen información de acuerdo con los estándares establecidos y el porcentaje de entidades que intercambian información con otras para trámites y/o servicios en línea utilizando intranet gubernamental, se tenía una meta del 100% para 2010; los porcentajes reales fueron de 69 y 19% respectivamente (8). El avance en el registro de información ha sido importante; no obstante, la desarticulación sigue teniendo niveles elevados.

Los prestadores de servicios, sean estos públicos o privados, tienen sus propios sistemas de información. Adicionalmente, los gobiernos locales tienen sus propios sistemas y plataformas de recopilación y gestión de datos.

2.3 MARCO TEÓRICO

2.3.1 Aspectos universales respecto a auditoria. Se puede afirmar que auditoría es la recopilación y evaluación de datos sobre información cuantificable de una entidad económica para determinar e informar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe ser realizada por una persona competente e independiente[5]. Competente porque debe ser un perito en el tema, independiente porque tanto debe ser externo a la entidad como autónomo cognoscitivamente.

[5] ARENS, Alvin A. Auditoria Un Enfoque Integral.6 Ed. México: Prentice Hall, 1996.

Objetivos generales de una auditoria de sistemas.

- "Seguridad de personal, datos, hardware, software e instalaciones.
- Conocer la situación actual del área de informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Asegurar una mayor integridad, confiabilidad y confidencialidad de la información mediante la recomendación de seguridades y controles.
- Incrementar la satisfacción de los usuarios de los sistemas computarizado.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riegos en el uso de tecnologías de información.
- Decisión de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los sistemas de información"[6].

2.3.2 Tipos de auditoria[7]. Existe tres tipos de auditorías básicas: auditorias de estado financieros, auditorias operacionales y auditorias de cumplimiento.

Auditorias de Estados Financieros

Se lleva a cabo una auditoria de estados financieros para determinar si el conjunto de los estados financieros (verificando la información cuantificable) se presentan de acuerdo con los criterios especificados. Por lo general, estos criterios son los principios de la contabilidad generalmente aceptados aunque también es común realizar auditorías de estados financieros que hayan sido preparados utilizando la base de efectivo y alguna otra base de contabilidad apropiada para la compañía. Los estados financieros comúnmente incluidos son el estado de posición financiera (Balance), el estado de resueltos y el estado de flujo de efectivo, incluyendo las notas correspondientes.

El supuesto tras una auditoria de estados financieros es que los utilizaran diferentes grupos para diferentes propósitos. Por lo tanto, es más eficiente hacer que un auditor realice una auditoría y saque conclusiones en las que puedan confiar todos los usuarios, en lugar de que cada usuario realice su propia auditoria. Si un usuario cree que la auditoría general no proporciona suficiente información para sus propósitos, el usuario tiene opción de obtener más datos. Por ejemplo, en una auditoria general de una empresa se puede obtener suficiente información financiera para un banquero que esté considerando un

[6] NARANJO, Alicia. Objetivos Generales de una auditoria de sistemas. Disponible en internet: http://anaranjo.galeon.com/objetiv_audi.htm Consultado: Abril de 2013

[7] ARENS, Alvin A. Auditoria Un Enfoque Integral.6 Ed. México: Prentice Hall, 1996.

préstamo para la compañía; pero una sociedad que considere una fusión con dicha empresa quizás también desee conocer el costo de reposición de los activos fijos y otra información pertinente para la decisión. La sociedad puede utilizar sus propios auditores para obtener información adicional.

Auditorias Operacionales

Una auditoria operacional es una revisión de cualquier parte del proceso y métodos de operación de una compañía con el propósito de evaluar su eficiencia y eficacia. Al término de una auditoria operacional, es común que la administración espere algunas recomendaciones para mejorar sus operaciones. Un ejemplo de una auditoria operacional es evaluar la eficiencia y precisión del procesamiento de una nómina en un sistema de cómputo recién instalado. Otro ejemplo, en donde se sentirán menos capacitados los contadores, seria en evaluar la eficiencia, precisión y satisfacción del cliente en la distribución de cartas y paquetes que hace una compañía de Federal Express.

Debido a las diversas áreas en que se evalúa la eficiencia operacional, es imposible caracterizar la realización de una auditoria operacional común y corriente. En una compañía, el auditor podría evaluar la pertinencia y suficiencia de la información que utiliza la administración para tomar decisiones sobre la adquisición de activos fijos; en tanto que en una compañía diferente, el auditor podría evaluar la eficiencia del flujo de documentos en el proceso de ventas. En las auditorias operacionales, los análisis no se limitan a la contabilidad. En ellos se puede incluir la evaluación de la estructura de una compañía, las operaciones de cómputo, los métodos de producción, la comercialización y cualquier otra área en la que esté capacitado el auditor.

La realización de una auditoria operacional y los resultados informados se definen con menos facilidad que cualquiera de los otros dos tipos de auditorías. La eficiencia y efectividad de las operaciones son más difíciles de evaluar objetivamente que el cumplimiento o presentación de estados financieros de acuerdo con los principios de contabilidad generalmente aceptados; y el establecer criterios para evaluar la información cuantificable en una auditoria operacional es un asunto sumamente subjetivo. En este sentido, la auditoria operacional se parece mucho más a la consultoría en administración que a lo que se considera generalmente como auditoria. La auditoría operacional ha aumentado en importancia desde la década pasada.

Auditorias de Cumplimiento

El propósito de una auditoria de cumplimiento es determinar si el auditado está cumpliendo con algunos procedimientos, reglas o reglamentos específicos que fije alguna autoridad superior. En una auditoria de cumplimiento para una empresa privada podría incluirse el determinar si el personal de contabilidad está siguiendo los procedimientos que ha prescrito el contralor de la compañía, el análisis de los niveles de salarios para cumplir con la leyes del salario mínimo o examinar los convenios contractuales con banqueros y otros prestamistas para asegurarse que la compañía está cumpliendo con los requisitos legales. En la auditoria de entidades gubernamentales, como distritos escolares, se verifica de forma amplia su cumplimiento debido a la extensa reglamentación por parte de autoridades gubernamentales superiores. En casi todos los organismos privados y no lucrativos, existen políticas prescritas, convenios contractuales y requerimientos legales que quizá requieran una auditoria de cumplimiento.

Es común que los resultados de las auditorias de cumplimiento sean informados a alguna persona que esté dentro del aérea que se está auditando en lugar de a un grupo amplio de usuarios. La administración, más que los usuarios externos, es el principal grupo interesado en el grado de cumplimiento con ciertos procedimientos y reglamentos prescritos. Por ende, gran parte del trabajo de este tipo lo realizan los auditores empleados por las mismas áreas. Existen excepciones. Cuando una empresa desea determinar si las personas u organismos que están obligados a seguir sus requerimientos contrata al auditor. Un ejemplo, son las auditorías a los contribuyentes para verificar si están cumpliendo con la leyes sobre impuestos federales, y en este caso el gobierno contrata al auditor para que audite las declaraciones de impuestos de los contribuyentes. Los CP son quienes realizan en gran medida las auditorias de cumplimiento de los programas que reciben subvenciones federales.

Auditoría Interna

La auditoría interna es una actividad independiente y objetiva basada en la filosofía de agregar valor para el mejor funcionamiento de una entidad, es exclusivamente realizada por personal profesional vinculado a la organización, los cuales tienen como objetivo primordial examinar y evaluar la adecuada y eficaz aplicación de los Sistemas de Control Interno. Para posteriormente proponer recomendaciones a las no conformidades encontradas.

Auditoría Externa

La auditoría externa es el examen crítico, sistemático y detallado de un sistema de información de una unidad de la empresa, realizado por personal profesional que no está vinculado a la organización. Los cuales utilizan técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera dicho sistema.

2.3.3 Identificación del objeto de estudio. En las organizaciones existe una filosofía la cual consiste en el viejo axioma divide y vencerás, es la razón por la cual las institución están subdividas en diferentes departamentos; y el Hospital Universitario Departamental de Nariño no es la excepción. En el departamento de sistemas del hospital se llevan a cabo un sin número de actividades las cuales requieren de un profundo grado de organización de parte de sus dirigentes; estas se alcanzan con políticas, normas y la previa definición de las actividades y un excelente manejo del personal en este departamento.

Por las razones anteriormente expuestas se hace necesario que los dirigentes de departamentos de sistemas tanto en organizaciones públicas o privadas y aún más en empresas prestadoras de servicios de salud en Colombia, que dentro de sus políticas administrativas se incluyan auditorias de sistemas periódicamente con el objeto de mejorar la calidad de la organización según sea su modelo de negocio.

2.3.3.1 Definición de alcance y objetivos[8]. El alcance de la Auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias, y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones del alcance de la Auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del informe final. Las personas que realizan la Auditoría han de conocer con mayor exactitud posible los objetivos a los que su tarea debe llegar. Debe conocer los deseos y pretensiones del cliente de forma que las metas fijadas puedan ser cumplidas. EL

[8]Auditores y asesores en contabilidad y sistemas. Alcance de la Auditoria Informática. Disponible en Internet: http://www.oocities.org/espanol/audiconsystem/auditori.htm Consultado: Marzo de 2013

alcance a definir con precisión el entorno y los límites en que va a desarrollar la Auditoría, se complementa con los objetivos de esta. El alcance ha de figurar expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

2.3.3.2 Estudio inicial del entorno auditable[9]. Para realizar el estudio inicial del entorno auditable ha de inspeccionarse las funciones y actividades generales del sistema de información, tales como: infraestructura tecnológica y software. Para su realización el auditor debe conocer lo siguiente:

Organización

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

Organigrama: El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

Relaciones Jerárquicas y funcionales entre órganos de la Organización: El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, si existe una deficiencia en cuanto a los rangos de la organización.

Las funcionales por el contrario, indican relaciones no estrictamente subordinables. Flujos de Información: Además de las corrientes verticales intradepartamentales, a estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales. Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio

[9]Archivos Auditoría en Sistemas. Estudio Inicial del Entorno Auditable. Disponible en Internet: http://archivosauditoria.blogspot.com/2009/11/estudio-inicial-del-entorno-auditable.html Consultado: Marzo de 2013

organigrama.

En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa. Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbación es en la organización.

Número de Puestos de Trabajo:

El equipo auditor comprobará que los nombres y los Puestos de Trabajo de la organización corresponden a las funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes. Esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

Número de Personas por Puesto de Trabajo:

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno Operacional:

El equipo de Auditoria informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

Situación Geográfica de los Sistemas:

Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.

Arquitectura y Configuración de Hardware y Software:

Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

Inventario de Hardware y Software:

El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPU, unidades de control local y remoto, periféricos de todo tipo, etc.

El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

Comunicación y Redes de Comunicación:

En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las Redes Locales de la Empresa.

Aplicaciones Bases de Datos y Ficheros:

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- Volumen, antigüedad y complejidad de las Aplicaciones.
- Metodología del Diseño.

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

Documentación:

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. La documentación de programas disminuye gravemente el mantenimiento de los mismos.

Cantidad y Complejidad de Bases de Datos y Ficheros:

El auditor recabará información de tamaño y características de las Bases de datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos. Estos datos proporcionan una visión aceptable de las características de la carga informática. Determinación de los recursos necesarios para realizar la Auditoria Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la Auditoria.

Recursos Materiales:

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.

Los Recursos Materiales del Auditor son de Dos Tipos:

Recursos Materiales Software:

Programas propios de la auditoria: Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

Monitores: Se utilizan en función del grado de desarrollo observado en la actividad técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

Recursos Materiales Hardware:

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado. Para lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

Recursos Humanos

Los recursos humanos son proporcionales a la cantidad auditable, a su vez las características y pericias del personal seleccionado obedece al enfoque a auditar. Las auditorias en general se llevan a cabo por personal especializado en áreas de auditorías o por otros profesionales que son facultados para auditar en su área de estudio.

2.3.3.3 Elaboración del programa de auditoria[10]. El programa de auditoría es un enunciado, lógicamente ordenado y clasificado, de los procedimientos de auditoría que han de emplearse, la extensión que se les ha de dar y la oportunidad en que se han de aplicar. Dado que los programas de auditoría se preparan anticipadamente en la etapa de planeación, estos pueden ser modificados en la medida en que se ejecute el trabajo, teniendo en cuenta los hechos concretos que se vayan observando.

El auditor deberá desarrollar y documentar un programa de auditoría que exponga la naturaleza, oportunidad y alcance de los procedimientos de auditoría planeados que se requieren para implementar el plan de auditoría global. El programa de auditoría sirve como un conjunto de instrucciones a los auxiliares involucrados en la auditoría y como medio para el control y registro de la ejecución apropiada del trabajo. El programa de auditoría puede también contener los objetivos de la auditoría para cada área y un presupuesto de tiempos en el que son presupuestadas las horas para las diversas áreas o procedimientos de auditoría.
Se acostumbra a elaborar un programa por cada sección a examinar, el cual debe incluir por lo menos el programa de trabajo en un sentido estricto y el programa adscrito al personal del trabajo a realizar. Cada programa de Auditoría permite el desarrollo del plan de trabajo general, pero a un nivel más analítico, aplicado a un área en particular.

[10] Conceptos Universales de Auditoría. Elaboración de los Programas de Auditoria. Disponible en internet: http://fccea.unicauca.edu.co/old/tgarf/tgarfse67.html Consultado: Marzo de 2013

El programa de auditoría contiene prácticamente la misma información que el plan de trabajo, pero difiere de este en que se le han adicionado columnas para el tiempo estimado, el tiempo real, la referencia al papel de trabajo donde quedó plasmada la ejecución del programa, la rúbrica de quien realizó cada paso y la fecha del mismo.

Por medio de cada programa de auditoría, el auditor adquiere control sobre el desarrollo del examen, pues estos además de ser una guía para los asistentes sirven para efectuar una adecuada supervisión sobre los mismos, permitiendo también determinar el tiempo real de ejecución de cada procedimiento para compararlo con el estimado y así servir de pauta para la planeación de las próximas auditorías, así mismo, permite conocer en cualquier momento el estado de adelanto del trabajo, ayudando a la toma de decisiones sobre la labor pendiente por realizar.

Generalmente el programa de auditoría comprenderá una sección por cada área de los estados financieros que se examinan. Cada sección del programa de auditoría debe comprender:

- Una introducción que describa la naturaleza de las cuentas examinadas y resuma los procedimientos de contabilidad de la compañía.
- Una descripción de los objetivos de auditoría que se persiguen en la revisión de la sección.
- Una relación de los pasos de auditoría que se consideran necesarios para alcanzar los objetivos señalados anteriormente.

2.3.3.4 Ejecución de la Auditoria[11]. El propósito fundamental de esta etapa es recopilar las pruebas que sustenten las opiniones del auditor en cuanto al trabajo realizado, es la fase, por decir de alguna manera, del trabajo de campo, esta depende considerablemente del grado de profundidad con que se hayan realizado las dos etapas anteriores, en esta se elaboran los Papeles de Trabajo y las hojas de nota, instrumentos que respaldan excepcionalmente la opinión del auditor actuante.

[11] MANSO, Gerónimo. Etapas de una Auditoría de Sistemas. Disponible en Internet: http://www.geronet.com.ar/?p=48 Consultado: Marzo de 2013

2.3.3.4.1 Elaboración del informe final. En esta etapa el Auditor se dedica a formalizar en un documento los resultados a los cuales llegaron los auditores en la Auditoría ejecutada y demás verificaciones vinculadas con el trabajo realizado.

Comunicar los resultados al máximo nivel de dirección de la entidad auditada y otras instancias administrativas, así como a las autoridades que correspondan, cuando esto proceda.

El informe parte de los resúmenes de los temas y de las Actas de Notificación de los Resultados de Auditoría que se vayan elaborando y analizando con los auditados, respectivamente, en el transcurso de la Auditoría.

La elaboración del informe final de Auditoría es una de las fases más importante y compleja de la Auditoría, por lo que requiere de extremo cuidado en su confección.

El informe de Auditoría debe tener un formato uniforme y estar dividido por secciones para facilitar al lector una rápida ubicación del contenido de cada una de ellas.

El informe de Auditoría debe cumplir con los principios siguientes:

- Que se emita por el jefe de grupo de los auditores actuantes.
- Por escrito.
- Oportuno.
- Que sea completo, exacto, objetivo y convincente, así como claro, conciso y fácil de entender.
- Que todo lo que se consigna esté reflejado en los papeles de trabajo y que responden a hallazgos relevantes con evidencias suficientes y competentes.
- Que refleje una actitud independiente.
- Que muestre la calificación según la evaluación de los resultados de la Auditoría.
- Distribución rápida y adecuada.

2.3.4 Estándares regionales e internacionales de auditorías de sistemas[12]. La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información. La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

Dentro de estas normas o estándares se tienen los siguientes:

- "**COSO** (Sponsoring Organizations of the Treadway Commission), es denominado así, porque se trata de un trabajo que encomendó el Instituto Americano de Contadores Públicos, la Asociación Americana de Contabilidad, el Instituto de Auditores Internos que agrupa a alrededor de cincuenta mil miembros y opera en aproximadamente en cincuenta países, el Instituto de Administración y Contabilidad, y el Instituto de Ejecutivos Financieros. Ha sido hecho para uso de los consejos de administración de las empresas privadas en España y en los países de habla hispana. Ahí se resume muy bien lo que es control interno, los alcances, etc.

[12] Asociación de Auditoría y control de Sistemas de Información. Normas Generales Para la Auditoria de sistemas de Información. Disponible en Internet: http://galeon.com/auditoriaycont/niads.pdf Consultado: Marzo de 2013

El Presidente Ejecutivo doctor Salas Chaves, manifiesta que el tema es muy importante y debe ser incorporado dentro del programa de capacitación para los gerentes, para que sea un manual de consultas en los hospitales. Sesión Junta Directiva: 7131, artículo 8. 1997"[13].

➢ "El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993. ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general"[14].

➢ "I**SO** (International Organization for Standardization), siendo ésta una agencia internacional especializada con 91 países miembros cuyo objetivo es el de promover el desarrollo mundial de la estandarización. Esta agencia empezó a analizar el tema de Calidad en 1970 y estableció el comité técnico para el desarrollo de los estándares; antes de esto existían diferentes estándares nacionales e internacionales sobre los sistemas de calidad en diferentes industrias, los cuales no eran consistentes en su terminología y requerimientos. La primera razón para desarrollar los estándares ISO 9000 y su terminología estándar ISO 8402, fue la de armonizar todos los requerimientos genéricos sobre un sistema de calidad en un solo grupo de estándares internacionalmente aprobados. Los resultados del trabajo del Comité, fueron cinco estándares consistentes en una serie de documentos que delinean un sistema de calidad aprobado internacionalmente, los cuales fueron adoptados en 1987 y son los siguientes:

[13] BONILLA, Carmen. El Informe Coso. Disponible en Internet: http://www.gerencie.com/el-informe-coso.html Consultado: Marzo de 2013

[14] ICONTEC. Reglamento del Servicio de Normalización Nacional. Disponible en Internet:http://www.icontec.org.co/files/reglamento_de_normalizacion.pdf Consultado: Marzo de 2013

ISO 9000 (1987) Guía para la selección y uso de las normas de gestión y aseguramiento de la calidad.

ISO 9001 (1987) Sistemas de calidad. Modelo para el aseguramiento de la calidad en el diseño, desarrollo, producción, instalación y servicio"[15].

- "**COBIT** (Control Objectives Control Objectives for Information and related Technology) Es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de TI y mejorar los controles de TI. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Para ayudar a las organizaciones a satisfacer con éxito los desafíos de los negocios actualmente.

COBIT es un framework de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de T.I. que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

COBIT hace posible el desarrollo de una política clara y las buenas prácticas para los controles de T.I. a través de las organizaciones.

COBIT enfatiza en la conformidad a regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de la estructura COBIT.

La versión, COBIT 4.1, enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de TI., apoya el alineamiento con el negocio y simplifica la implantación de COBIT. Esta versión no invalida el trabajo efectuado con las versiones anteriores del COBIT, sino que puede ser empleado para mejorar el trabajo previo"[16].

---

[15] Administración de la Calidad. Diseño de sistemas de calidad total. Disponible en Internet:http://www.itch.edu.mx/academic/industrial/admoncalidad/unidad05.html Consultado: Marzo de 2013.

[16] DARTHSOUL. Cobit4.1. Disponible en Internet: http://www.chullohack.com/2009/07/31/cobit-4-1-en-espanol/ Consultado: Marzo de 2013

➢ "**COBIT 5** provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público"[17].

2.3.5 Herramientas y técnicas para la auditoría de sistemas

2.3.5.1 Entrevistas. Las entrevistas le proporcionan al auditor el conocimiento del personal auditado y como se están llevando a cabo las funciones en la organización, aunado a esto las entrevistas conllevan a lo siguiente:

➢ El auditor comienza a continuación las relaciones personales con el auditado.
➢ La entrevista es una de las actividades personales más importante del auditor; recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.
➢ interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

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

Se suele solicitar la compleción de cuestionarios que se envían a las personas concretas que el auditor cree adecuadas. Estos cuestionarios deben ser específicos para cada situación, y muy cuidados en su fondo y su forma.

[17] Archivo [pdf] COBIT 5, Un marco de negocio para el gobierno y gestion de las ti de la empresa.- Adobe Reader.p.13.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otros medios la información que aquellos impresos hubieran proporcionado.

Los checklist o listas de chequeo le son de gran ayuda al auditor ya que no le permiten omitir puntos específicos dentro del proceso de auditoría.
El auditor debe tener claro lo que se necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior.

- **Checklist binaria:** se realizan con preguntas de Si o No se califican: con 0 el puntaje más bajo con 1er puntaje más alto.

- **Checklist de rango:** se realizan con preguntas que maneja jerarquía es decir de lo general a lo particular. Permiten hacer un mejor sondeo de la entidad auditada. Ya que le permiten al auditor ahondar con preguntas "sencillas" en la organización. Estas son calificas con puntajes de 1 a 5 siendo uno el puntaje más bajo y cinco el puntaje más alto.

2.3.5.3 Trazas o Huellas[18]. Con frecuencia, el auditor debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en **productos Software** muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Estas Trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas.

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

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el

[18] SALAZAR, Hernández. Trazas y Huellas. Disponibles en Internet:http://www.angelfire.com/tx/rolas/audi/clase18_19feb_traza_softevi.htm Consultado: Marzo de 2013

fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de contabilidad, en donde se encuentra la producción completa de aquél, y los Log de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general. Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

2.3.5.3.1 Software de interrogación. Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados

solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.

2.3.6 Estándar utilizado en la auditoria del HUDN[19]. El COBIT fue lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

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

[19] ACOSTA, Mario. Norma Cobit. Disponible en Internet: http://nyxmario7.wordpress.com/2010/06/01/norma-cobit/ Consultado: Abril de 2013

Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

Usuarios:

La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido. Los Responsables de TI: para identificar los controles que requieren en sus áreas.

Características del COBIT:

- Orientado al negocio
- Alineado con estándares y regulaciones “de facto”
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

Principios: El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.
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.

Aunado a lo anterior el COBIT contiene 4 pilares o dominios, 34 procesos y 210 objetivos de control. Los cuatro dominios son:

- Planear y organizar
- Adquirir e implantar
- Entregar y dar soporte
- Monitorear y evaluar

Criterios

Planear y Organizar: Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).

Adquirir e Implementar: Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes. Proporciona las soluciones y las pasa para convertirlas en servicios.

Entregar y Dar Soporte: Cubre la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Recibe las soluciones y las hace utilizables por los usuarios finales.

Monitorear y Evaluar: Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Monitorear todos los procesos para asegurar que se sigue la dirección provista.

2.3.6.1 Criterios de Información de COBIT.

La Efectividad: tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

La Eficiencia: consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

La Confidencialidad: se refiere a la protección de información sensitiva contra revelación no autorizada.

La Integridad: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

La Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

El Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

La Confiabilidad: se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

2.4 MARCO CONCEPTUAL

2.4.1 Auditoria. Es un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con las actividades que se desarrollan en una entidad pública o privada. El fin del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que

le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso[20].
Del párrafo anterior se tiene que:

Sistemático: que se realiza algorítmicamente es decir que hay que llevar un conjunto de pasos para solucionar la auditoria.

2.4.1.1 Auditar. Auditar significa inspeccionar que la gestión económica de una organización, respecto a la información financiera, operacional, administrativa y sistematizada es correcta y confiable. Aunado a lo anterior es cerciorarse que los acontecimientos actuales, se han realizado de la forma como fueron planeados. Que cumplan con todos los reglamentos ya sean de aspectos jurídicos o en general.

2.4.1.2 Técnicas de Auditoria[21]. Son los métodos prácticos de investigación y prueba que el contador público utiliza para comprobar la razonabilidad de la información financiera que le permita emitir su opinión profesional.

Técnicas de auditoría, son todos los métodos prácticos de investigación y prueba que el contador público utiliza para corroborar su opinión profesional.
Las técnicas de auditoría son las siguientes:

Estudio General: Apreciación sobre la fisonomía o características generales de la empresa, de sus estados financieros de los rubros y partidas importantes, significativas o extraordinaria. Esta apreciación se hace aplicando el juicio profesional del Contador Público, que basado en su preparación y experiencia, podrá obtener de los datos e información de la empresa que va a examinar, situaciones importantes o extraordinarias que pudieran requerir atención especial.

Análisis. Clasificación y agrupación de los distintos elementos individuales que forman una cuenta o una partida determinada, de tal manera que los grupos constituyan unidades homogéneas y significativas.

---

[20] CLAVIJO, Lina maría. Auditoría General y Control Interno. Disponible en internet: http://auditoriaycontrol2010b.blogspot.com/2010/08/definicion-generica-de-auditoria.html Consultado: Abril de 2013

[21] CASTREJÓN, Lilian. Técnicas de Auditoria. Disponible en internet: http://www.gestiopolis.com/recursos/documentos/fulldocs/fin1/tecaudito.htm Consultado: Abril de 2013

El análisis generalmente se aplica a cuentas o rubros de los estados financieros para conocer cómo se encuentran integrados y son los siguientes:

- **Análisis de saldos**

Existen cuentas en las que los distintos movimientos que se registran en ellas son compensaciones unos de otros, por ejemplo, en una cuenta de clientes, los abonos por pagos, devoluciones, bonificaciones, etc., son compensaciones totales o parciales de los cargos por ventas. En este caso, el saldo de la cuenta está formado por un neto que representa la diferencia entre las distintas partidas que se registraron en la cuenta. En este caso, se pueden analizar solamente aquellas partidas que forman parte del saldo de la cuenta. El detalle de las partidas residuales y su clasificación en grupos homogéneos y significativos, es lo que constituye el análisis de saldo.

- **Análisis de movimientos**

En otras ocasiones, los saldos de las cuentas se forman no por compensación de partidas, sino por acumulación de ellas, por ejemplo, en las cuentas de resultados; y en algunas cuentas de movimientos compensados, puede suceder que no sea factible relacionar los movimientos acreedores contra los movimientos deudores, o bien. Por razones particulares no convenga hacerlo. En este caso, el análisis de la cuenta debe hacerse por agrupación, conforme a conceptos homogéneos y significativos de los distintos movimientos deudores y acreedores que constituyen el saldo de la cuenta.

Inspección. Examen físico de los bienes materiales o de los documentos, con el objeto de cerciorarse de la existencia de un activo o de una operación registrada o presentada en los estados financieros.

En diversas ocasiones, especialmente por lo que hace a los saldos del activo, los datos de la contabilidad están representados por bienes materiales, títulos de crédito u otra clase de documentos que constituyen la materialización del dato registrado en la contabilidad.

En igual forma, algunas de las operaciones de la empresa o sus condiciones de trabajo, pueden estar amparadas por títulos, documentos o libros especiales, en los cuales, de una manera fehaciente quede la constancia de la operación realizada. En todos estos casos, puede comprobarse la autenticidad del saldo de la cuenta, de la operación realizada o de la circunstancia que se trata de

comprobar, mediante el examen físico de los bienes o documentos que amparan el activo o la operación.

Confirmación. Obtención de una comunicación escrita de una persona independiente de la empresa examinada y que se encuentre en posibilidad de conocer la naturaleza y condiciones de la operación y, por lo tanto, confirmar de una manera válida.

Esta técnica se aplica solicitando a la empresa auditada que se dirija a la persona a quien se pode la confirmación, para que conteste por escrito al auditor, dándole la información que se solicita y puede ser aplicada de diferentes formas:

Positiva. Se envían datos y se pide que contesten, tanto si están conformes como si no lo están. Se utiliza este tipo de confirmación, preferentemente para el activo.

Negativa. Se envían datos y se pide contestación, sólo si están inconformes. Generalmente se utiliza para confirmar pasivo o a instituciones de crédito.

Investigación. Obtención de información, datos y comentarios de los funcionarios y empleados de la propia empresa.

Con esta técnica, el auditor puede obtener conocimiento y formarse un juicio sobre algunos saldos u operaciones realizadas por la empresa. Por ejemplo, el auditor puede formarse su opinión sobre la contabilidad de los saldos de deudores, mediante informaciones y comentarios que obtenga de los jefes de los departamentos de crédito y cobranzas de la empresa.

Declaración. Manifestación por escrito con la firma de los interesados, del resultado de las investigaciones realizadas con los funcionarios y empleados de la empresa.

Esta técnica, se aplica cuando la importancia de los datos o el resultado de las investigaciones realizadas lo ameritan.

Aun cuando la declaración es una técnica de auditoría conveniente y necesaria, su validez está limitada por el hecho de ser datos suministrados por personas que

participarlo en las operaciones realizadas o bien, tuvieron injerencia en la formulación de los estados financieros que se está examinando.

Certificación. Obtención de un documento en el que se asegure la verdad de un hecho, legalizado por lo general, con la firma de una autoridad.

Observación. Presencia física de cómo se realizan ciertas operaciones o hechos. El auditor se cerciora de la forma como se realizan ciertas operaciones, dándose cuenta ocularmente de la forma como el personal de la empresa las realiza. Por ejemplo, el auditor puede obtener la convicción de que los inventarios físicos fueron practicados de manera satisfactoria, observando cómo se desarrolla la labor de preparación y realización de los mismos.

Cálculo. Verificación matemática de alguna partida. Hay partidas en la contabilidad que son resultado de cómputos realizados sobre bases predeterminadas. El auditor puede cerciorarse de la corrección matemática de estas partidas mediante el cálculo independiente de las mismas.

En la aplicación de la técnica del cálculo, es conveniente seguir un procedimiento diferente al ampliado originalmente en la determinación de las partidas.

Por ejemplo, el importe de los intereses ganados originalmente calculados sobre la base de cómputos mensuales sobre operaciones individuales, se puede comprobar por un cálculo global aplicando la tasa de interés anual al promedio de las inversiones del periodo.

2.4.2 Sistema. Sistema es un conjunto de elementos interdependientes, que interactúan entre si formando un todo organizado.

2.4.2.2 Sistemas de información. Desde el punto de vistas computacional un SI es un conjunto de elementos conectados para la administración de datos e información, que posteriormente genera salidas que coadyuvan a la toma de decisiones.

Las actividades fundamentales de un SI son:

- **Captura de datos:** la cual consiste en seleccionar de una lista, datos pertinentes entre varios datos según corresponda, o captura automática a través de láser.

- **Procesar datos:** Se toman las entradas y las convierte en salida mediante el algoritmo que maneje el sistema de Información.

2.4.2.2 Auditoria de un sistema de información. Es la indagación que se le realiza a un SI, respecto a entradas, proceso y salidas. Posteriormente se presentan conclusiones y recomendaciones para tratar de corregir las falencias existentes.

Los aspectos generales a evaluar, son:

1. Eficiencia en los recursos informáticos.
2. Importancia de la información.
3. Confianza de los controles establecidos.
4. Seguridad física y lógica

2.4.3 Aspectos de calidad de SI

2.4.3.1 Funcionalidad. Es la capacidad de un producto software para suministrar las funciones que satisfacen las necesidades establecidas, cuando el software se utiliza bajo condiciones específicas.

2.4.3.2 Confiabilidad. Es la capacidad de un producto software para conservar su desempeño en diferente lapso de tiempo. Aunado a lo anterior se logra información adecuada en el momento adecuado para proporcionar informes y reportes en el menor tiempo posible.

2.4.3.3 Eficiencia. La eficiencia en SI hace referencia a la capacidad que tiene el sistema para otorgar un desempeño adecuado, con respecto a los recursos utilizados, es decir es la utilización óptima de los recursos del sistema.

2.4.3.4 Usabilidad. Esta se refiere a la capacidad que proporciona el SI para ser entendido por el usuario final.

2.4.3.5 Portabilidad. Se refiere a la capacidad que posee un SI para ser utilizados en diferentes plataformas.

2.4.3.6 Cumplimiento. Hace referencia a los medio para adquirir la información en tiempo pasado, presente y futuro.

2.4.4 Estructura Organizacional

2.4.4.1 Planeación Estratégica Informática[22]. Se define de la reunión de los administradores de la organización, donde analizan tanto información interna como externa para proporcionar a los interesados un dictamen de la misma es decir el estado en que se encuentra actualmente la institución. Durante el proceso se establecen los factores críticos de soporte a las estrategias de la empresa y sus métricas, de tal manera que la inversión en tecnología pueda ser fácilmente justificable.

La planeación estratégica se rige por siete elementos fundamentales que son:

I. Preparación Para la Planeación

Antes de iniciar el proceso, hay que definir y preparar claramente lo siguiente:

a) Compromiso de la organización a seguir el proceso completo y aplicar resultados La metodología o pasos a seguir, los marcos de tiempo, el presupuesto requerido.
b) Quien será el responsable interno del proceso y productos.
c) Cuales miembros de la organización deben participar y en que paso participan.
d) Necesidades de información previa.
e) Definir las prioridades en lo referente a área geográfica, temas, especies, etc., en los que la organización concentrará sus esfuerzos (este paso debe ajustarse según el contexto específico de cada organización con referente a su área de producción de bienes o servicios).

[22] UNIPAMPLONA. Planeación Estratégica de los Sistemas de Información. Disponible en internet: https://docs.google.com/document/d/1RrIAiiAB0p46X9PPAF4iDVa97ZxGnZRxoUkwrF2UBtw/edit?pli=1 Consultado: Abril de 2013

II. Desarrollo de la Visión y Misión

La Visión es una meta a largo plazo y refleja cómo se ve la empresa en ese futuro, es como un sueño que se pretende alcanzar. Su conocimiento por todos los miembros de la organización es muy importante porque significa que todos saben para dónde se va.

La Misión es la razón de ser de la empresa. Orienta a todos los empleados para que las decisiones que se tomen no se salgan del rumbo y representen esfuerzos perdidos. Su conocimiento debe ser por todos los miembros de la empresa.

III. Análisis de la Situación Actual Externa (Amenazas, Oportunidades; también se conoce como POAM: perfil de oportunidades y amenazas del medio).

IV. Análisis Interno de la Organización (Fortalezas y Debilidades; también se conoce como PCI: perfil de capacidad institucional).

Al conjunto de Debilidades, Oportunidades, Fortalezas y Amenazas, se les conoce con el nombre de DOFA y resumen lo que es el Diagnóstico Situacional.

V. Definición de Metas y Objetivos Estratégicos. Seleccionar el Portafolio o Cartera de Proyectos. Estos están dirigidos a prevenir las amenazas, disminuir las debilidades, mantener las fortalezas y aprovechar las oportunidades.

VI. Integración de la Estrategia con el Plan Financiero y Otras Áreas de la Organización (Producción, Mercadeo y Talento humano).

VII.Implementación de la Estrategia: Es la parte operativa y en donde se diseñan, implementan, monitorean, y evalúan los proyectos.

3. METODOLOGÍA

3.1 ETAPAS DE AUDITORIA

3.1.1 ETAPA I: Fase de conocimiento. En esta etapa se recolectó la información utilizando diversas técnicas e instrumentos como entrevistas, observación directa y cuestionarios.

✓ Realizar visitas al hospital para conocer el sitio donde funciona el módulo, la información que se procesa y los usuarios que lo utilizan.
✓ Realizar entrevistas al administrador y usuarios acerca del funcionamiento del sistema y el módulo inventarios del sistema de información.
✓ Diseñar y aplicar cuestionarios para identificar algunas fallas, vulnerabilidades y riesgos en el manejo, la administración y funcionamiento del sistema.

3.1.2 ETAPA II: fase de análisis y evaluación de riesgos. Se realizó la identificación de vulnerabilidades, riesgos y amenazas, y su valoración con respecto a la probabilidad e impacto mediantes la utilización del COBIT (Control objectives for information and related technology).

✓ Identificar las vulnerabilidades, riesgos y amenazas existentes en el sistema.
✓ Valorar los riesgos según la escala definida para la probabilidad e impacto.

3.1.3 ETAPA III: fase de ejecución de pruebas. Se elaboró un plan de pruebas que fue realizado y ejecutado para verificar y conformar los riesgos que han sido detectados.

✓ Elaborar un plan de pruebas que será aplicado para buscar evidencias de las fallas y riesgos existentes.
✓ Realizar comparaciones o benchmarking con otros sistemas que estén funcionando adecuadamente.
✓ Ejecutar pruebas sobre el sistema y el módulo de inventarios del sistema de información para verificar su funcionalidad.

3.1.4 ETAPA IV: fase de presentación informe final. Se realizó el informe detallado con las fallas encontradas en el módulo, y se proponen soluciones para establecer un plan de mejoramiento que ayude a optimizar el funcionamiento general del módulo.

✓ Realizar la matriz de hallazgos donde se evidencian los riesgos, la causa y los recursos afectados
✓ Elaborar el dictamen de la auditoria que se confrontará con los auditados para hacer descargos
✓ Elaborar el informe final que será presentado al ingeniero que solicitó la auditoria y a los directivos.
✓ Proponer estrategias de mejoramiento para optimizar el funcionamiento del módulo y el sistema.

3.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.2.1 Fuentes primarias. Las fuentes primarias en el desarrollo de esta auditoría se poseen las siguientes:

➢ Entrevistas, dirigidas al personal del departamento de sistemas y todas las áreas involucradas con la trazabilidad de la información del módulo de inventario.
➢ Ejecución de los cuestionarios en todas las área incluidas en el módulo de inventario.
➢ Manuales, que estén relacionados con el módulo de inventarios del DGH.
➢ Módulo de inventario del DGH.
➢ Base de datos relacionada con el módulo de inventario.

3.2.2 Fuentes secundarias. Para el desarrollo de este proyecto de auditoría, se contó con la vasta gama de libros referenciales y la web, por lo anterior se logró consultar temas relacionados con auditorías a sistemas de información, aspectos legales para la constitución de inventarios en empresas estatales y la administración de estos.

4. DESARROLLO DEL PROYECTO

4.1 ARCHIVO PERMANENTE

4.1.1 Ambiente general de la empresa

4.1.1.1 Nombre de la empresa

Hospital Universitario Departamental de Nariño E.S.E

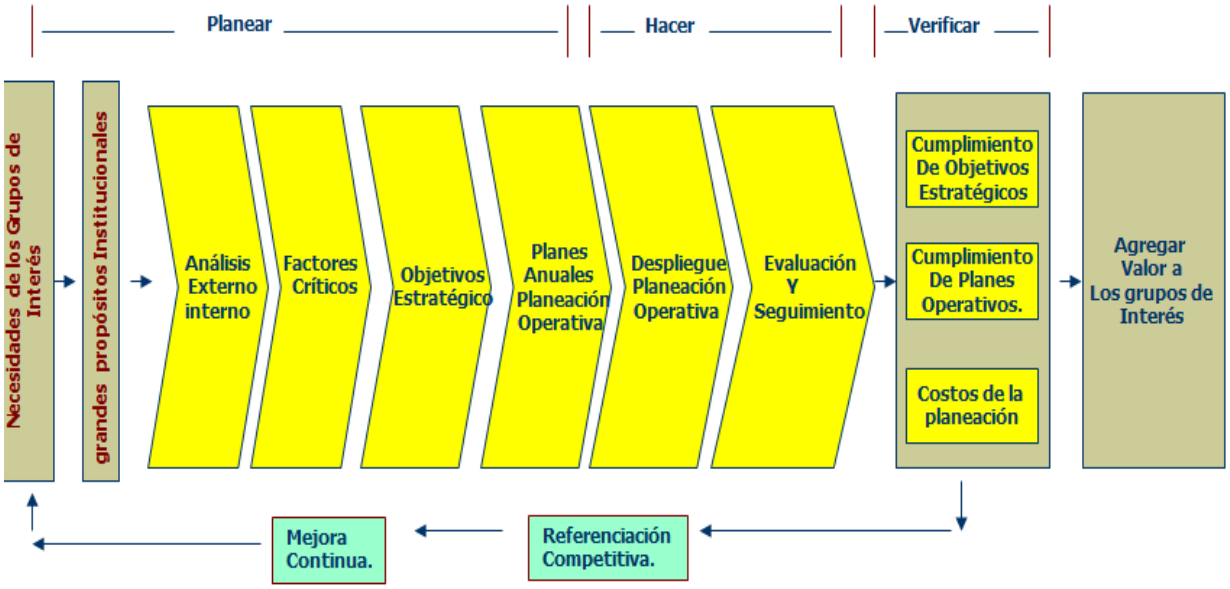
4.1.1.2 Entorno del hospital universitario departamental de Nariño[23]. El Hospital Universitario Departamental de Nariño E.S.E., es la única organización de la red pública de nivel III de la región, funciona desde el 15 de diciembre de 1975 y en octubre de 1990, mediante Resolución del Ministerio de Salud No. 14676.El Hospital Departamental de Nariño es clasificado como un organismo para atención de nivel III. A partir del 10 de diciembre de 1994, se constituye en una Empresa social del Estado por ordenanza 067 expedida en la Asamblea Departamental de Nariño, proyectándose con los avances de la Ciencia, la Tecnología y la Gerencia Moderna a la comunidad del Sur Occidente del País.

Enmarca su accionar actual, circunscrito al entorno del Sistema de la Seguridad Social en Salud, fortaleciendo su estructura organizacional y empresarial frente al reto de este milenio enfocado hacia el III y IV nivel de complejidad. Actualmente el Hospital Departamental de Nariño E.S.E. cambia su razón social por Hospital Universitario Departamental de Nariño E.S.E.

[23] Biblioteca virtual, hospital universitario departamental de Nariño, Disponible en: http://www.hosdenar.gov.co, (Citado el 13 de mayo de 2013

4.1.1.3 Sistema de gestión estratégica

Figura 1. Gestión estratégica



Fuente: Hospital universitario departamental de Nariño E.S.E.

4.1.1.4 Recursos técnicos del módulo de inventario. El Hospital universitario Departamental de Nariño, cuenta con 376 computadoras los cuales se encuentran distribuidos en todas las áreas de la entidad, con el objeto de suplir las actividades que se presentan en el hospital.

Dentro del módulo de inventario se encuentran implantado 16 computadoras y 12 impresoras que tienen relación directa o indirecta con el modulo.

4.1.2 Organización administrativa

4.1.2.1 Área de información y sistemas. El Hospital Universitario Departamental Nariño E.S.E. se encuentra ubicado en Calle 22 No 7-93 Parque Bolívar. El Hospital se encuentra regido por las siguientes políticas de las cuales las más connotadas son:

De Calidad: El compromiso es superar las necesidades y expectativas de nuestros clientes internos y externos, contribuyendo positivamente al mejoramiento de la calidad de vida de los habitantes de nuestra región, para lo cual decidimos establecer y mejorar continuamente un Sistema de Gestión Integral para la Calidad, garantizando una atención humanizada, dentro del marco legal existente, con competencia técnica y científica, oportunidad e información clara y real a nuestros usuarios y su familia, involucrando en este propósito el desarrollo integral y participativo tanto de los trabajadores como de nuestros proveedores, logrando con ello el crecimiento de la organización.

Ambiental: Los esfuerzos estarán dirigidos hacia la preservación del medio ambiente, y hacia la creación de una cultura eficiente que estandarice nuestras acciones, bajo la aplicación de un sistema integral de administración ambiental.

De Salud Ocupacional: El Hospital Universitario Departamental de Nariño E.S.E. declara su especial interés, por la protección de la integridad de sus trabajadores, usuarios y comunidad que directa o indirectamente están involucrados en sus procesos a través de la identificación de los factores de riesgo en los puestos de trabajo, su evaluación y control de estos, asignando recursos necesarios e implementando procesos de mejoramiento continuo orientados a la prevención de accidentes de trabajo y enfermedades profesionales dentro del marco legal.

De Equidad: Es compromiso de la Organización, impulsar la equidad entre hombres y mujeres asegurando la igualdad de oportunidades, favoreciendo la equidad de género, así como el cumplimiento de la ley en cuanto fortalecer ambientes de trabajo en donde se respete la dignidad de la personas.

Administrativa: Modernizar sistemas y procesos acorde con la normatividad, alienando la estructura a la estrategia y a la cultura deseada.

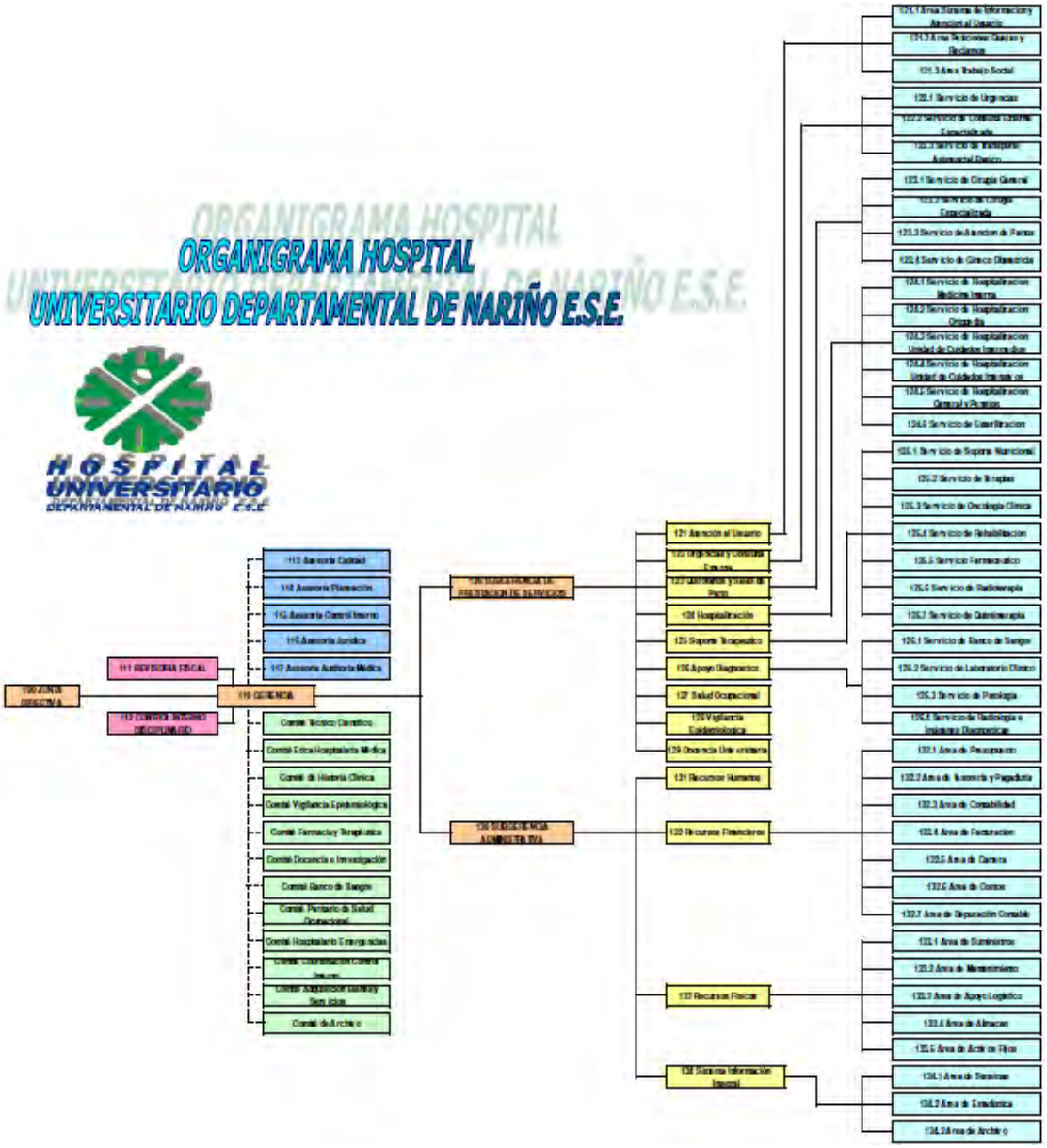
Laboral: Proporcionar condiciones adecuadas de trabajo para mejorar la calidad de vida de sus trabajadores y propiciar su desarrollo.

Social: Promover la activa participación de comunidad en los procesos de desarrollo organizacional y coadyuvar a la creación de estilos de vida saludables con actividades de promoción en nuestro nivel de complejidad.

Económica Financiera: Administrar correctamente los bienes y recursos para el óptimo beneficio empresarial y lograr la eficiencia operativa al menor costo. Las anteriores políticas tienen como objetivo cumplir al código buen gobierno del Hospital Universitario Departamental de Nariño.

4.1.2.2 Organización jerárquica de la institución E.S.E.

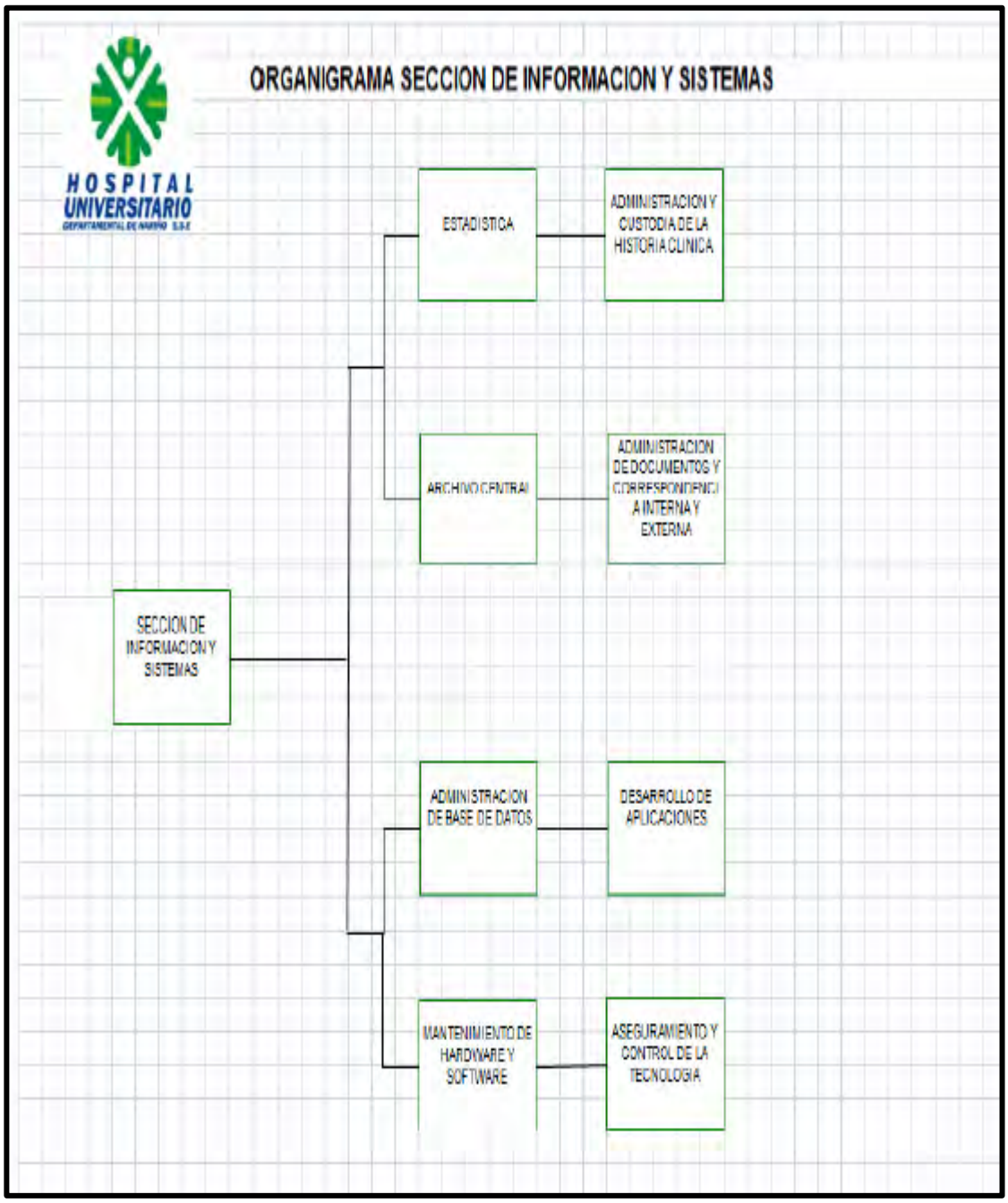
Figura 2. Organigrama del HUDN



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.1.2.3 Organigrama del área de sistemas

Figura 3. Sistema



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.1.3 Cargos y funciones dentro del hospital universitario departamental de Nariño. Los cargos y funciones de la auditoria al módulo de inventario del Sistema de Información en el Hospital Universitario Departamental de Nariño están soportados por:

MANUAL DE FUNCIONES DEL HUDN. El cual se anexa al documento final de este proyecto.

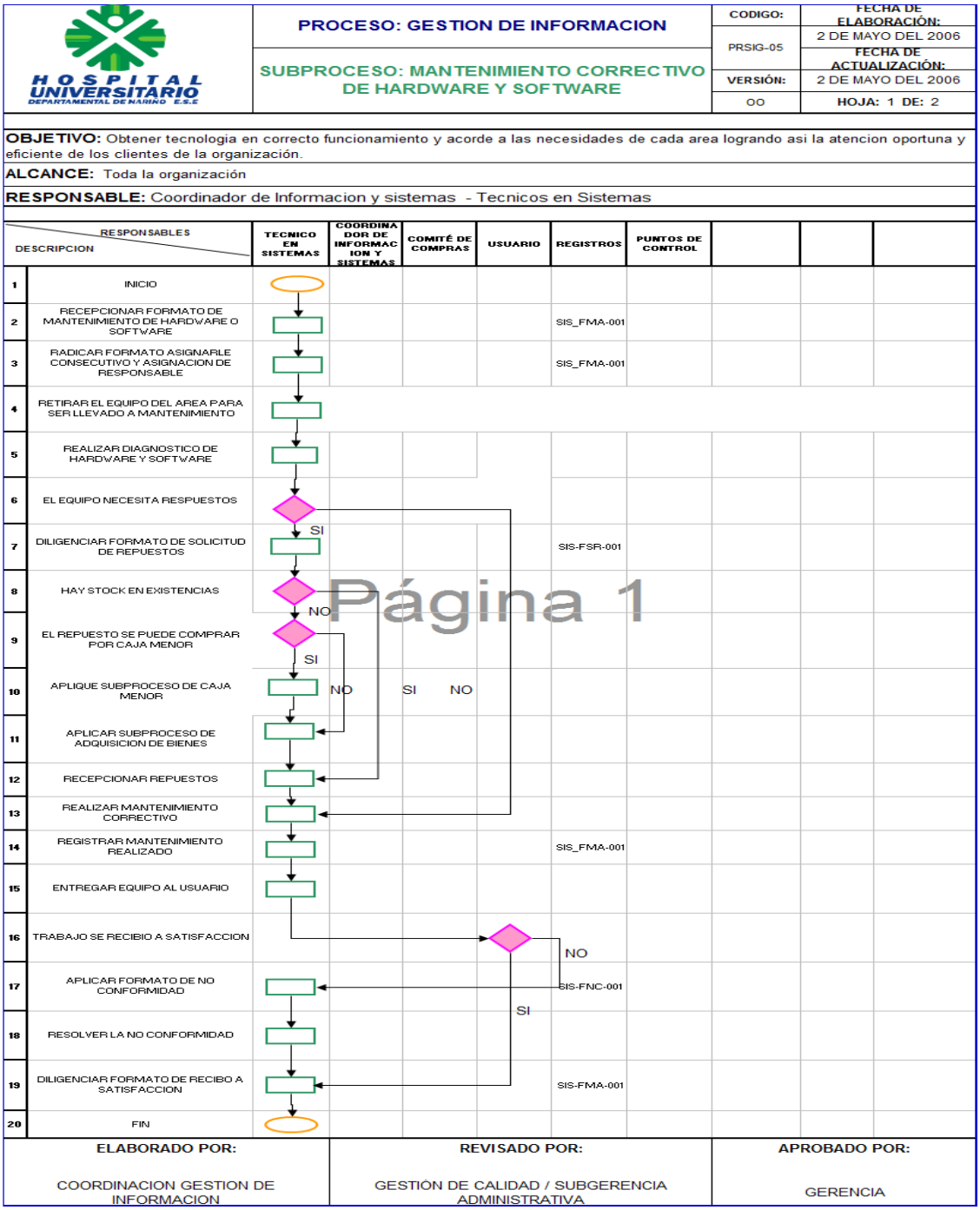
4.1.4 Personal de soporte del área sistemas del HUDN

Personal	Funciones
Ingeniero Orlando Argoty	Garantizar el respaldo de la información registrada en los equipos de cómputo de la institución con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.
Técnicos Sistemas William Solarte, Jhony Meneses	Mantener los equipos de cómputo en buenas condiciones de funcionamiento con el fin de garantizar el normal desempeño de los procesos y la vida útil de los equipos.
Ingeniero Orlando García, Ricardo Villota	Brindar información confiable, oportuna a los clientes externos e internos de la organización que la requieran.
Técnico Jeider Quintero, Manuel Vinueza	Dar soluciones informáticas a las áreas de la organización que las requieran, con base en los requerimientos de información de cada una de ellas, con el fin de lograr sistematizar sus procesos obteniendo un adecuado tiempo de respuesta en la atención de sus clientes.
Coordinador de Gestión de Información Roberto Yánez	Garantizar un sistema de información confiable mediante un proceso de auditoría que permita, administrar y controlar por medio de una evaluación, al proveedor del Sistema de Información y aplicativos desarrollados por el mismo y los implantados por la organización.

Fuente: Hospital Universitario Departamental de Nariño E.S.E.

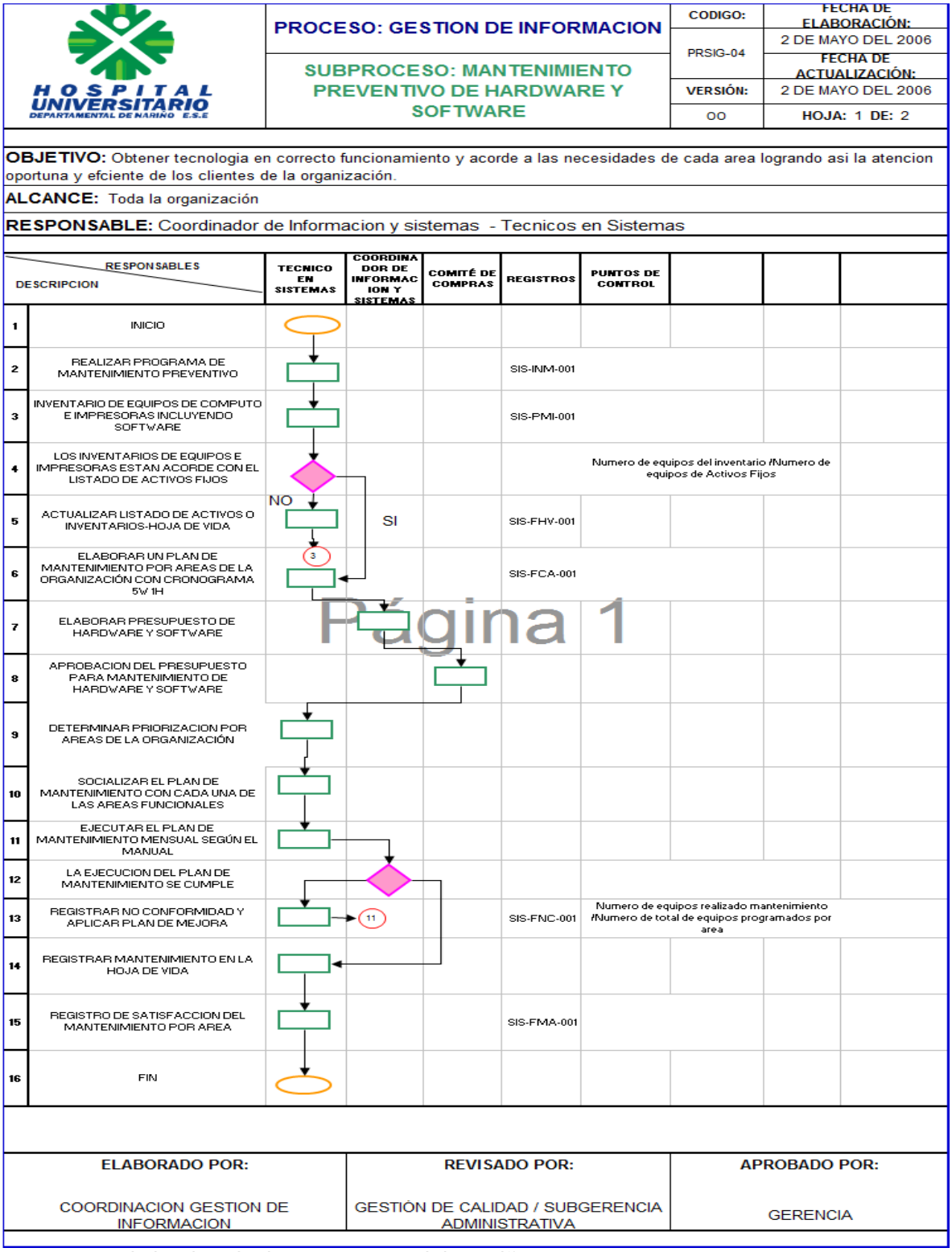
4.1.5 Diagramas del área de información y sistemas del hospital universitario departamental de Nariño.

Figura 4. Mantenimiento correctivo



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 5. Mantenimiento preventivo



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
		PRSIG-04	2 DE MAYO DEL 2006
	SUBPROCESO: MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		00	HOJA: 1 DE: 2

OBJETIVO: Obtener tecnologia en correcto funcionamiento y acorde a las necesidades de cada area logrando asi la atencion oportuna y efciente de los clientes de la organización.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	COMITÉ DE COMPRAS	REGISTROS	PUNTOS DE CONTROL
1	INICIO					
2	REALIZAR PROGRAMA DE MANTENIMIENTO PREVENTIVO				SIS-INM-001	
3	INVENTARIO DE EQUIPOS DE COMPUTO E IMPRESORAS INCLUYENDO SOFTWARE				SIS-PMI-001	
4	LOS INVENTARIOS DE EQUIPOS E IMPRESORAS ESTAN ACORDE CON EL LISTADO DE ACTIVOS FIJOS					Numero de equipos del inventario /Numero de equipos de Activos Fijos
5	ACTUALIZAR LISTADO DE ACTIVOS O INVENTARIOS-HOJA DE VIDA				SIS-FHV-001	
6	ELABORAR UN PLAN DE MANTENIMIENTO POR AREAS DE LA ORGANIZACIÓN CON CRONOGRAMA 5W 1H				SIS-FCA-001	
7	ELABORAR PRESUPUESTO DE HARDWARE Y SOFTWARE					
8	APROBACION DEL PRESUPUESTO PARA MANTENIMIENTO DE HARDWARE Y SOFTWARE					
9	DETERMINAR PRIORIZACION POR AREAS DE LA ORGANIZACIÓN					
10	SOCIALIZAR EL PLAN DE MANTENIMIENTO CON CADA UNA DE LAS AREAS FUNCIONALES					
11	EJECUTAR EL PLAN DE MANTENIMIENTO MENSUAL SEGÚN EL MANUAL					
12	LA EJECUCION DEL PLAN DE MANTENIMIENTO SE CUMPLE					
13	REGISTRAR NO CONFORMIDAD Y APLICAR PLAN DE MEJORA				SIS-FNC-001	Numero de equipos realizado mantenimiento /Numero de total de equipos programados por area
14	REGISTRAR MANTENIMIENTO EN LA HOJA DE VIDA					
15	REGISTRO DE SATISFACCION DEL MANTENIMIENTO POR AREA				SIS-FMA-001	
16	FIN					

NO

SI

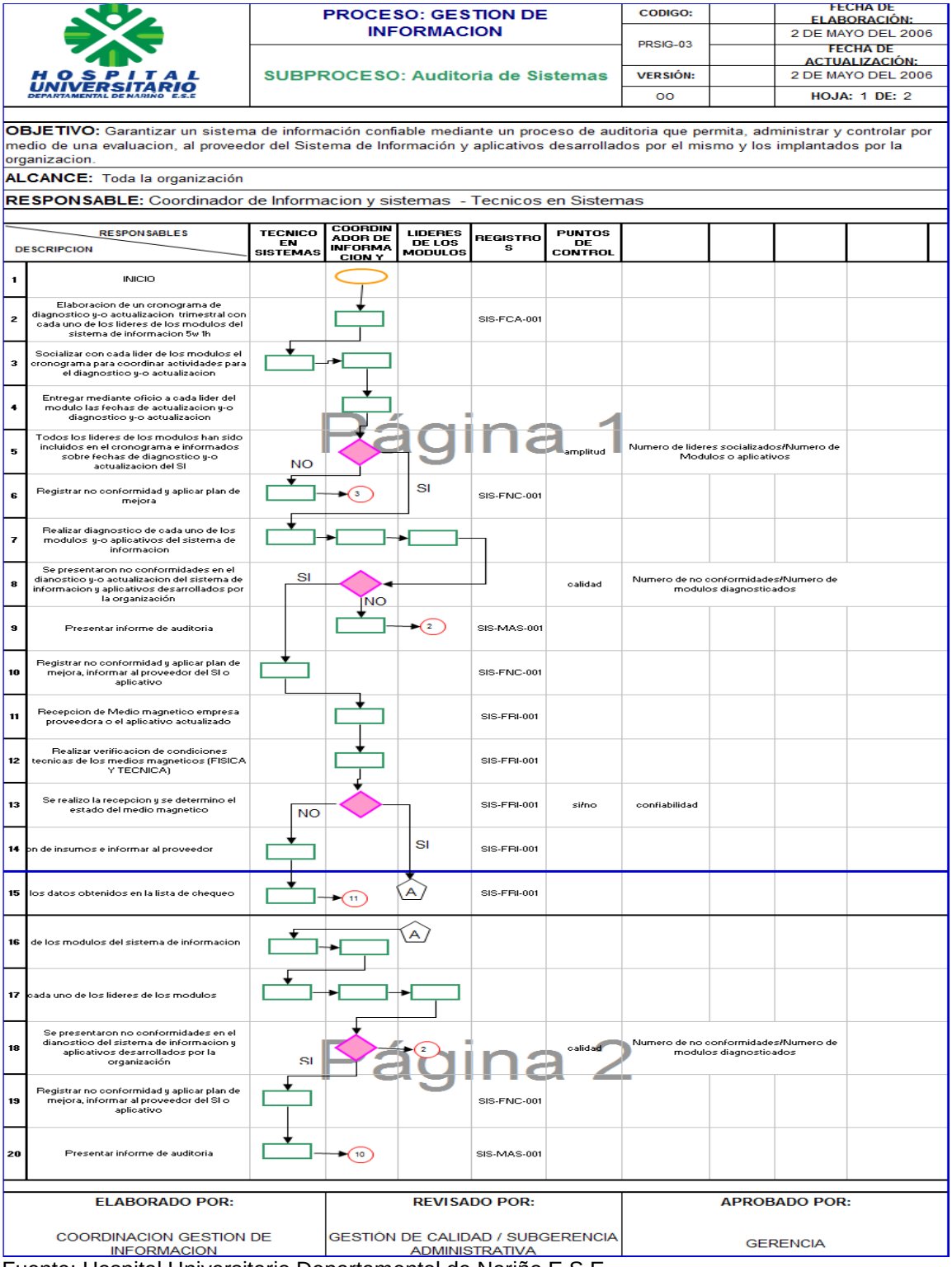
3

11

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COORDINACION GESTION DE INFORMACION	GESTIÓN DE CALIDAD / SUBGERENCIA ADMINISTRATIVA	GERENCIA

Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 6. Auditoria de sistemas



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE INFORMACION	CODIGO:		FECHA DE ELABORACIÓN:
		PRSIG-03		2 DE MAYO DEL 2006
	SUBPROCESO: Auditoria de Sistemas	VERSIÓN:		FECHA DE ACTUALIZACIÓN:
		OO		2 DE MAYO DEL 2006
				HOJA: 1 DE: 2

OBJETIVO: Garantizar un sistema de información confiable mediante un proceso de auditoria que permita, administrar y controlar por medio de una evaluacion, al proveedor del Sistema de Información y aplicativos desarrollados por el mismo y los implantados por la organizacion.

ALCANCE: Toda la organización

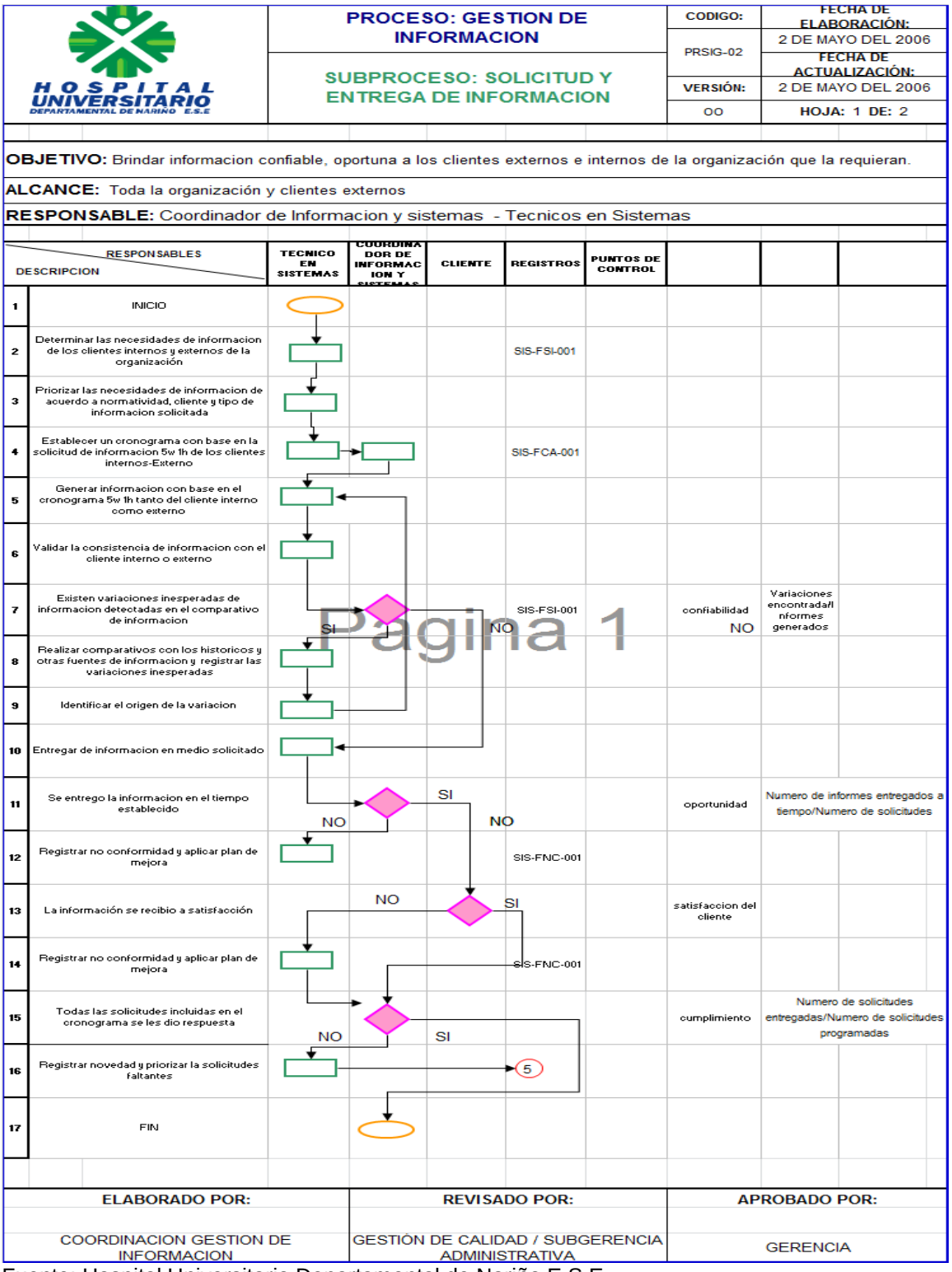
RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y	LIDERES DE LOS MODULOS	REGISTROS	PUNTOS DE CONTROL				
1	INICIO									
2	Elaboracion de un cronograma de diagnostico y-o actualizacion trimestral con cada uno de los lideres de los modulos del sistema de informacion 5w 1h				SIS-FCA-001					
3	Socializar con cada lider de los modulos el cronograma para coordinar actividades para el diagnostico y-o actualizacion									
4	Entregar mediante oficio a cada lider del modulo las fechas de actualizacion y-o diagnostico y-o actualizacion									
5	Todos los lideres de los modulos han sido incluidos en el cronograma e informados sobre fechas de diagnostico y-o actualizacion del SI					amplitud	Numero de lideres socializados/Numero de Modulos o aplicativos			
6	Registrar no conformidad y aplicar plan de mejora				SIS-FNC-001					
7	Realizar diagnostico de cada uno de los modulos y-o aplicativos del sistema de informacion									
8	Se presentaron no conformidades en el dianostico y-o actualizacion del sistema de informacion y aplicativos desarrollados por la organización					calidad	Numero de no conformidades/Numero de modulos diagnosticados			
9	Presentar informe de auditoria				SIS-MAS-001					
10	Registrar no conformidad y aplicar plan de mejora, informar al proveedor del SI o aplicativo				SIS-FNC-001					
11	Recepcion de Medio magnetico empresa proveedora o el aplicativo actualizado				SIS-FRI-001					
12	Realizar verificacion de condiciones tecnicas de los medios magneticos (FISICA Y TECNICA)				SIS-FRI-001					
13	Se realizo la recepcion y se determino el estado del medio magnetico				SIS-FRI-001	si/no	confiabilidad			
14	ón de insumos e informar al proveedor				SIS-FRI-001					
15	los datos obtenidos en la lista de chequeo				SIS-FRI-001					
16	de los modulos del sistema de informacion									
17	cada uno de los lideres de los modulos									
18	Se presentaron no conformidades en el dianostico del sistema de informacion y aplicativos desarrollados por la organización					calidad	Numero de no conformidades/Numero de modulos diagnosticados			
19	Registrar no conformidad y aplicar plan de mejora, informar al proveedor del SI o aplicativo				SIS-FNC-001					
20	Presentar informe de auditoria				SIS-MAS-001					

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COORDINACION GESTION DE INFORMACION	GESTIÓN DE CALIDAD / SUBGERENCIA ADMINISTRATIVA	GERENCIA

Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 7. Solicitud y entrega



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
		PRSIG-02	2 DE MAYO DEL 2006
	SUBPROCESO: SOLICITUD Y ENTREGA DE INFORMACION		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

OBJETIVO: Brindar informacion confiable, oportuna a los clientes externos e internos de la organización que la requieran.

ALCANCE: Toda la organización y clientes externos

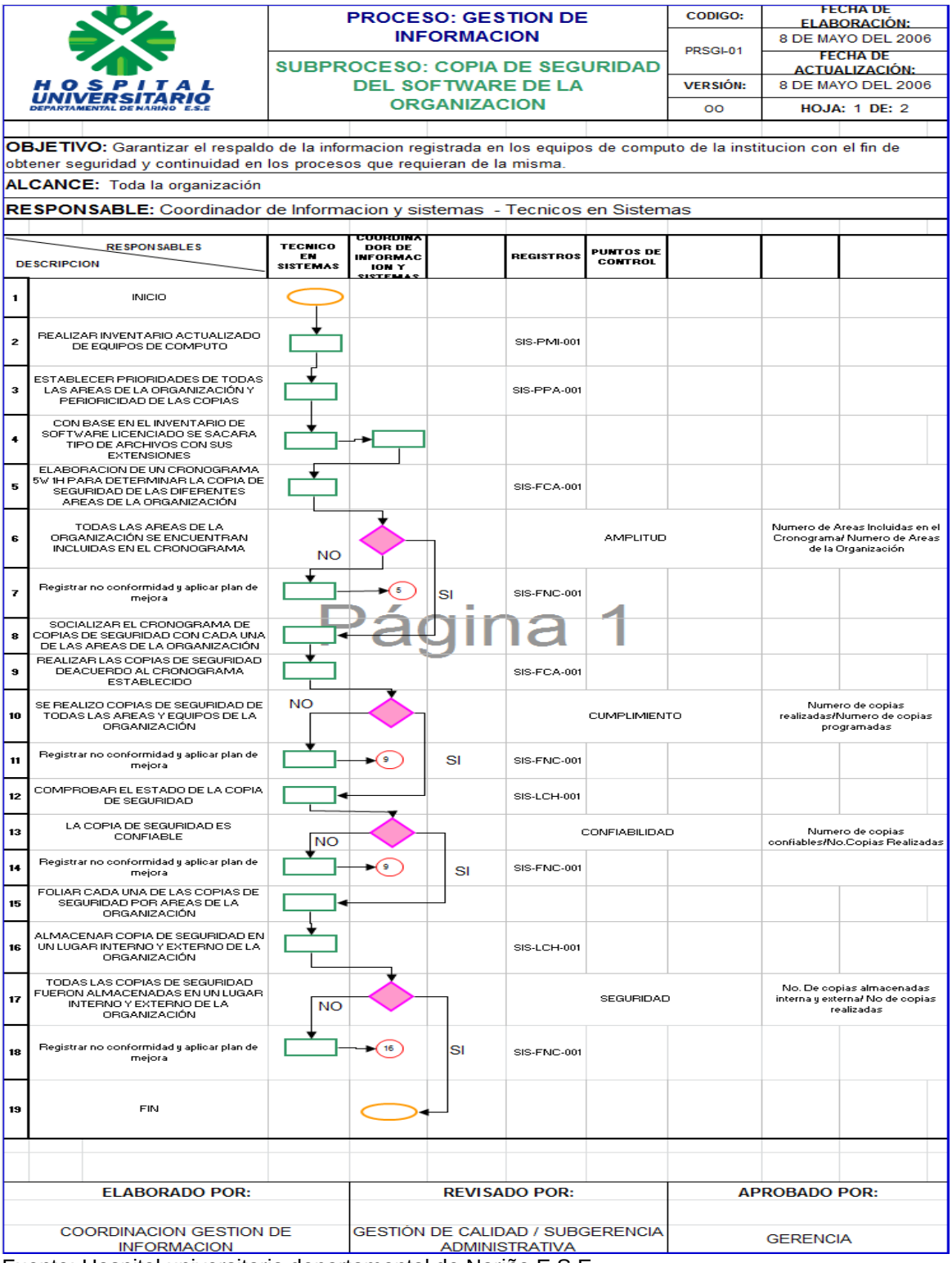
RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	CLIENTE	REGISTROS	PUNTOS DE CONTROL			
1	INICIO								
2	Determinar las necesidades de informacion de los clientes internos y externos de la organización				SIS-FSI-001				
3	Priorizar las necesidades de informacion de acuerdo a normatividad, cliente y tipo de informacion solicitada								
4	Establecer un cronograma con base en la solicitud de informacion 5w 1h de los clientes internos-Externo				SIS-FCA-001				
5	Generar informacion con base en el cronograma 5w 1h tanto del cliente interno como externo								
6	Validar la consistencia de informacion con el cliente interno o externo								
7	Existen variaciones inesperadas de informacion detectadas en el comparativo de informacion				SIS-FSI-001		confiabilidad	Variaciones encontradas/Informes generados	
8	Realizar comparativos con los historicos y otras fuentes de informacion y registrar las variaciones inesperadas								
9	Identificar el origen de la variacion								
10	Entregar de informacion en medio solicitado								
11	Se entrego la informacion en el tiempo establecido						oportunidad	Numero de informes entregados a tiempo/Numero de solicitudes	
12	Registrar no conformidad y aplicar plan de mejora				SIS-FNC-001				
13	La información se recibio a satisfacción						satisfaccion del cliente		
14	Registrar no conformidad y aplicar plan de mejora				SIS-FNC-001				
15	Todas las solicitudes incluidas en el cronograma se les dio respuesta						cumplimiento	Numero de solicitudes entregadas/Numero de solicitudes programadas	
16	Registrar novedad y priorizar la solicitudes faltantes								
17	FIN								

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COORDINACION GESTION DE INFORMACION	GESTIÓN DE CALIDAD / SUBGERENCIA ADMINISTRATIVA	GERENCIA

Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 8. Copia de seguridad



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
		PRSGI-01	8 DE MAYO DEL 2006
	SUBPROCESO: COPIA DE SEGURIDAD DEL SOFTWARE DE LA ORGANIZACION		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	8 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

OBJETIVO: Garantizar el respaldo de la informacion registrada en los equipos de computo de la institucion con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.

ALCANCE: Toda la organización

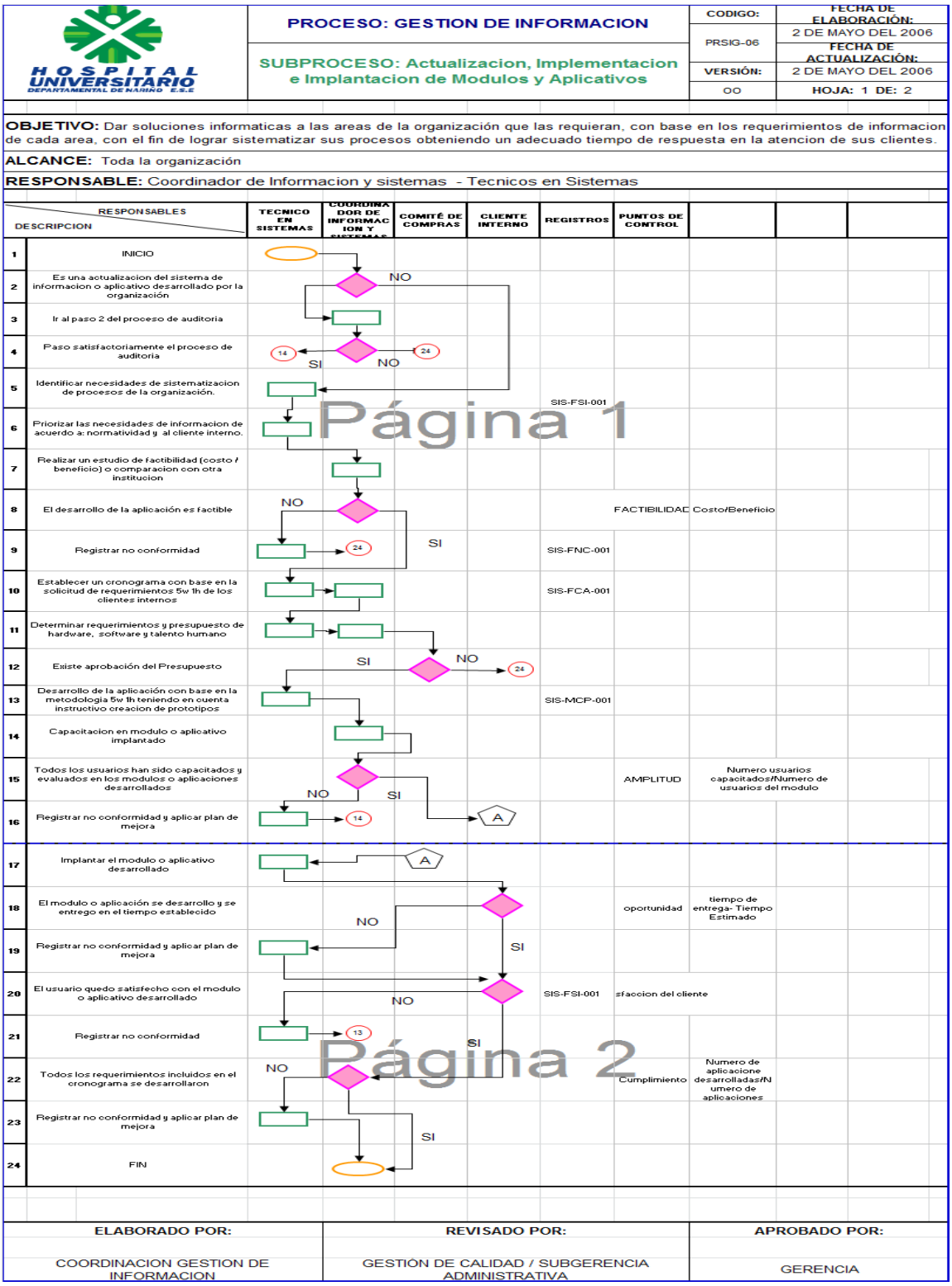
RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	REGISTROS	PUNTOS DE CONTROL			
1	INICIO							
2	REALIZAR INVENTARIO ACTUALIZADO DE EQUIPOS DE COMPUTO			SIS-PMI-001				
3	ESTABLECER PRIORIDADES DE TODAS LAS AREAS DE LA ORGANIZACIÓN Y PERIORICIDAD DE LAS COPIAS			SIS-PPA-001				
4	CON BASE EN EL INVENTARIO DE SOFTWARE LICENCIADO SE SACARA TIPO DE ARCHIVOS CON SUS EXTENSIONES							
5	ELABORACION DE UN CRONOGRAMA 5W 1H PARA DETERMINAR LA COPIA DE SEGURIDAD DE LAS DIFERENTES AREAS DE LA ORGANIZACIÓN			SIS-FCA-001				
6	TODAS LAS AREAS DE LA ORGANIZACIÓN SE ENCUENTRAN INCLUIDAS EN EL CRONOGRAMA	NO		AMPLITUD			Numero de Areas Incluidas en el Cronograma/ Numero de Areas de la Organización	
7	Registrar no conformidad y aplicar plan de mejora	5	SI	SIS-FNC-001				
8	SOCIALIZAR EL CRONOGRAMA DE COPIAS DE SEGURIDAD CON CADA UNA DE LAS AREAS DE LA ORGANIZACIÓN							
9	REALIZAR LAS COPIAS DE SEGURIDAD DEACUERDO AL CRONOGRAMA ESTABLECIDO			SIS-FCA-001				
10	SE REALIZO COPIAS DE SEGURIDAD DE TODAS LAS AREAS Y EQUIPOS DE LA ORGANIZACIÓN	NO		CUMPLIMIENTO			Numero de copias realizadas/Numero de copias programadas	
11	Registrar no conformidad y aplicar plan de mejora	9	SI	SIS-FNC-001				
12	COMPROBAR EL ESTADO DE LA COPIA DE SEGURIDAD			SIS-LCH-001				
13	LA COPIA DE SEGURIDAD ES CONFIABLE	NO		CONFIABILIDAD			Numero de copias confiables/No.Copias Realizadas	
14	Registrar no conformidad y aplicar plan de mejora	9	SI	SIS-FNC-001				
15	FOLIAR CADA UNA DE LAS COPIAS DE SEGURIDAD POR AREAS DE LA ORGANIZACIÓN							
16	ALMACENAR COPIA DE SEGURIDAD EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN			SIS-LCH-001				
17	TODAS LAS COPIAS DE SEGURIDAD FUERON ALMACENADAS EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN	NO		SEGURIDAD			No. De copias almacenadas interna y externa/ No de copias realizadas	
18	Registrar no conformidad y aplicar plan de mejora	16	SI	SIS-FNC-001				
19	FIN							

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COORDINACION GESTION DE INFORMACION	GESTIÓN DE CALIDAD / SUBGERENCIA ADMINISTRATIVA	GERENCIA

Fuente: Hospital universitario departamental de Nariño E.S.E.

Figura 9. Actualización e implementación



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.2 ARCHIVO CORRIENTE

Este archivo está compuesto por documentos y pales directamente relacionados con el desarrollo del proyecto.

4.2.1 Memorando de planeación. Este define algorítmicamente el desarrollo de la auditoria y sus objetivos.

4.2.1.1 Objetivo general. Evaluar la eficiencia y eficacia del módulo de inventario del Sistema de Información del Hospital Universitario Departamental de Nariño para coadyuvar en su buen funcionamiento.

4.2.1.2 Objetivos específicos

- Identificar el funcionamiento de las entradas al módulo de inventario.
- Analizar las salidas de informes generados por el módulo de inventario.
- Efectuar un seguimiento riguroso a toda la trazabilidad de la información del módulo de inventario.
- Establecer estrategias de mejoramiento al módulo de inventario del Hospital Universitario Departamental de Nariño.

4.2.1.3 Alcance. La información es el activo más importante dentro de cualquier organización. Cada vez existe un mayor requerimiento de información fidedigna en el entorno hospitalario, que se presenta de varios tipos como es la información externa, interna, administrativa y de gestión. Esta es manejada en el módulo de inventario del sistema de información integrado del Hospital Universitario de Nariño, El cual le permite controlar los ingresos y salidas de mercancías por cualquier concepto, además permite establecer estadísticas, costos, rentabilidad y movimientos de cada uno de los productos.

En el transcurso de la auditoria se encamino a evaluar las entradas y las salidas correspondientes al módulo de Inventario, que permiten controlar los medicamentos así como los insumos manejados por el hospital, inspeccionando de forma eficaz y eficiente la administración de insumos y medicinas. Este módulo posee interfaces directas con los módulos de Facturación y Presupuesto.
Durante el transcurso de la auditoria se realizó la evaluación de las entradas y las salidas al Módulo de Inventario junto con las interfaces que este tiene relación, es decir se verificó la trazabilidad de todos y cada uno de los movimientos que este Módulo maneja.

Las entradas al módulo de inventario del DGH del HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO, son:

Orden de Compra
Remisión de Entrada
Comprobante de entrada
Devolución de Ventas
Devolución de Suministro
Solicitudes

Las salidas del módulo de inventario del DGH del HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO, son:

Suministro de Paciente
Remisión de Salida
Pedido y Factura
Devolución de Compras
Solicitud de pedido

4.2.14 Justificación. En la actualidad las organizaciones manipulan una serie de productos necesarios para ejecutar sus actividades de manera adecuada, para ello se requiere manejar estos recursos del mejor modo posible y la mejor forma de hacerlo es utilizando la técnica del inventario; que permite registrar todos los movimientos de los almacenes, mediante el establecimiento de normas y parámetros para cada producto, lo cual resulta muy importante dentro de una organización, ya que permite controlar eficientemente la recepción, registro, conservación, distribución de los productos y materiales.

En el Hospital Universitario Departamental de Nariño el módulo de inventario se encarga de administrar todos los movimientos de entrada y de salida, tanto de medicamentos como de insumos necesarios para una óptima prestación del servicio de esta organización, motivo por el cual no deben existir errores.

Con base en las razones expuestas es muy importante realizar auditorías continuas al módulo de inventario, ya que estas, permitirán identificar fortalezas y debilidades de la trazabilidad de la información manejada por este módulo.

Además lo más importante de realizar una auditoría al módulo de Inventario del DGH, está basado en que ayudará al mejoramiento continuo de la calidad hospitalaria, que establece un aumento en la prestación de los servicios, haciéndolos más eficientes y eficaces.

4.2.1.5 Metodología. La metodología para la el desarrollo del proyecto consta de las siguientes etapas:

ETAPA I: Fase de Conocimiento

En esta etapa se recolectó la información utilizando diversas técnicas e instrumentos como entrevistas, observación directa y cuestionarios.

✓ Realizar visitas al hospital para conocer el sitio donde funciona el módulo, la información que se procesa y los usuarios que lo utilizan
✓ Realizar entrevistas al administrador y usuarios acerca del funcionamiento del sistema y el módulo inventarios del sistema de información.
✓ Diseñar y aplicar cuestionarios para identificar algunas fallas, vulnerabilidades y riesgos en el manejo, la administración y funcionamiento del sistema.

ETAPA II: Fase de Análisis y Evaluación de Riesgos

Se realizó la identificación de vulnerabilidades, riesgos y amenazas, y su valoración con respecto a la probabilidad e impacto mediantes la utilización del COBIT (modelo para auditoría y control de sistemas de información).

✓ Identificar las vulnerabilidades, riesgos y amenazas existentes en el sistema
✓ Valorar los riesgos según la escala definida para la probabilidad e impacto

ETAPA III: Fase de Ejecución de Pruebas

Se elaboró un plan de pruebas que serán realizadas y ejecutadas para verificar y conformar los riesgos que han sido detectados.

✓ Elaborar un plan de pruebas que será aplicada para buscar evidencias de las fallas y riesgos existentes.
✓ Realizar comparaciones o benchmarking con otros sistemas que estén funcionando adecuadamente.
✓ Ejecutar pruebas sobre el sistema y el módulo de inventarios del sistema de información para verificar su funcionalidad.

ETAPA IV: Fase de presentación Informe Final

Se realizó el informe detallado con las fallas encontradas en el módulo, y se proponen soluciones para establecer un plan de mejoramiento que ayude a optimizar el funcionamiento general del módulo.

✓ Realizar la matriz de hallazgos donde se evidencian los riesgos, la causa y los recursos afectados.
✓ Elaborar el dictamen de la auditoria que se confrontará con los auditados para hacer descargos.
✓ Elaborar el informe final que será presentado al ingeniero que solicitó la auditoria y a los directivos.
✓ Proponer estrategias de mejoramiento para optimizar el funcionamiento del módulo y el sistema.

4.2.1.6 Recursos

Recursos tecnológicos

➢ 1Computador de mesa: Sistema operativo Windows Xp, procesador Intel Pentium D, 1 GB memoria RAM, disco duro de 160 GB y quemador de DVD.
➢ 1Computador Portátil: Sistema operativo Windows 7, procesador Intel Core i3, 3 GB memoria RAM, disco duro de 320 GB y quemador de DVD.

Software:

➢ Programa de aplicación dinámica gerencial(**DGH**)
➢ Acceso total al Módulo de Inventario del **DGH**.

Talento humano:

➢ Auditores responsables para esta auditoría: Jorge Alexis Portilla Vargas.
Denis Colunge Belalcázar.

Otros recursos:

- Grabadora de video y audio.
- Cámara fotográfica.
- 2 Memorias USB.
- Elementos de papelería (hojas, lapiceros, blocks de apuntes, lápiz y otros).
- Fotocopias.

4.2.2 Programa de auditoria. Para la ejecución de la auditoria al módulo de inventarios del sistema de información (**DGH**) del Hospital Universitario Departamental de Nariño E.S.E, se utilizó la metodología COBIT (Control Objetives for Information and related Technology) de ISACA (Information System Audit and Control Asociation), que cubre 210 objetivos de control clasificados en 4 dominios y 34 procesos. De los cuales se aplican los siguientes:

4.2.2.1 Dominio A- planear y organizar (PO). Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

4.2.2.1.1 Definir la arquitectura de la información (PO2). Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio enfocándose en el establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos

- **PO2.1 Modelo de arquitectura de información empresarial**

Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, rentable oportuna segura y tolerante a fallas.

- **PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos**

Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita la compartición de elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.

- **PO2.3 Esquema de clasificación de datos**

Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o encripción.

- **PO2.4 IT Administración de la Integridad**

Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

4.2.2.1.2 Determinar la dirección tecnológica (PO3). Contar con sistemas aplicativos estándar, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros enfocándose en la definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.

- **PO3.1 Planeación de la dirección tecnológica**

Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

- **PO3.2 Plan de infraestructura tecnológica**

Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de

sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

- **PO3.3 Monitoreo de tendencias y regulaciones futuras**

Establecer un proceso para monitorear las tendencias ambientales del sector industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

- **PO3.4 Estándares tecnológicos**

Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

- **PO3.5 Consejo de arquitectura**

Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se relacionan con la arquitectura de la información.

4.2.2.1.3 Administrar recursos humanos de TI (PO7). Administrar los recursos humanos de TI para formar personas competentes y motivadas para crear y entregar servicios de TI enfocándose en la contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos.

- **PO7.1 Reclutamiento y Retención del Personal**

Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales

- **PO7.2 Competencias del Personal**

Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

- **PO7.3 Asignación de Roles**

Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. Los términos y condiciones de empleo deben enfatizar la responsabilidad del empleado respecto a la seguridad de la información, al control interno y al cumplimiento regulatorio. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

- **PO7.4 Entrenamiento del Personal de TI**

Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

- **PO7.5 Dependencia Sobre los Individuos**

Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

- **PO7.6 Procedimientos de investigación del personal**

Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada o crítica sea la función y aplicar a los empleados, contratistas y proveedores.

- **PO7.7 Evaluación del desempeño del empleado**

Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

- **PO7.8 Cambios y terminación de trabajo**

Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Realizar la transferencia del conocimiento, reasignar responsabilidades y eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

4.2.2.1.4 Evaluar y administrar los riesgos de TI (PO9). Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio enfocándose en la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.

- **PO9.1 Alineación de la Administración de Riesgos de TI y del Negocio**

Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización.

- **PO9.2 Establecimiento del Contexto del Riesgo**

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

- **PO9.3 Identificación de Eventos**

Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

- **PO9.4 IT Evaluación de Riesgos**

Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales determinar de forma individual, por categoría y con base en el portafolio.

- **PO9.5 Respuesta a los Riesgos**

Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

- **PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos**

Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

4.2.2.2 Dominio B - adquirir e implementar (AI). Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

4.2.2.2.1 Adquirir y mantener infraestructura tecnológica (AI3). Adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI enfocándose en proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

- **AI3.1 Plan de adquisición de infraestructura tecnológico**

Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.

- **AI3.2 Protección y disponibilidad del recurso de infraestructura**

Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura monitorear y evaluar su uso.

- **AI3.3 Mantenimiento de la infraestructura**

Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

- **AI3.4 Ambiente de prueba de factibilidad**

Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad.

4.2.2.2.2 Instalar y acreditar soluciones y cambios (AI7). Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación enfocándose en probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libres de errores, y planear las liberaciones a producción.

- **AI7.1 Entrenamiento**

Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.

- **AI7.2 Plan de prueba**

Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito. El plan considera la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal. Con base en la evaluación de riesgos de fallas en el sistema y en la implantación, el plan deberá incluir los requerimientos de prueba de desempeño, stress, de usabilidad, piloto y de seguridad.

- **AI7.3 Plan de implantación**

Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de versiones (release), construcción de paquetes de versiones, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la versión y documentación de cambios. El plan deberá también incluir medidas de respaldo/ y vuelta atrás.

- **AI7.4 Ambiente de prueba**

Establecer un ambiente de prueba separado para pruebas. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas. tener presentes los procedimientos para garantizar que los datos utilizados en el ambiente de prueba sean representativos de los datos (se limpian si es necesario)

que se utilizarán eventualmente en el ambiente de operación. Proporcionar medidas adecuadas para prevenir la divulgación de datos sensibles. La documentación de los resultados de las pruebas archivar.

- **AI7.5 Conversión de Sistema y Datos**

Garantizar que los métodos de desarrollo de la organización, contemplen para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfaces con otros sistemas, procedimientos, documentación de sistemas, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se desarrolla y mantiene una pista de auditoría de los resultados previos y posteriores a la conversión. Los propietarios del sistema llevan a cabo una verificación detallada del proceso inicial del nuevo sistema para confirmar una transición exitosa.

- **AI7.6 Prueba de Cambios**

Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular. Las pruebas paralelas o piloto se consideran parte del plan. Los controles de seguridad se prueban y evalúan antes de la liberación, de manera que se pueda certificar la efectividad de la seguridad. Los planes de respaldo/vuelta atrás desarrollar y probar antes de transferir el cambio a producción.

- **AI7.7 Prueba final de Aceptación**

Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las pruebas deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba salvar para propósitos de pistas de auditoría y para pruebas futuras.

- **AI7.8 Promoción a Producción**

Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación. La gerencia debe requerir que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año.

- **AI7.9 Revisión Posterior a la Implantación**

Establecer procedimientos en línea con los estándares de gestión de cambios organizacionales para requerir una revisión posterior a la implantación como conjunto de salida en el plan de implementación.

4.2.2.3 Dominio C - entregar y dar soporte (DS). Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.

4.2.2.3.1 DS5 garantizar la seguridad de los sistemas (DS5). Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI. Enfocándose en el desarrollo de resistencia (resilience) en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.

- **DS5.1 Administración de la seguridad de TI**

Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

- **DS5.2 Plan de seguridad de TI**

Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas

en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

- **DS5.3 Administración de identidad**

Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

- **DS5.4 Administración de cuentas del usuario**

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

- **DS5.5 Pruebas, vigilancia y monitoreo de la seguridad**

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

- **DS5.6 Definición de incidente de seguridad**

Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

- **DS5.7 Protección de la tecnología de seguridad**

Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

- **DS5.8 Administración de llaves criptográficas**

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

- **DS5.9 Prevención, detección y corrección de software malicioso**

Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

- **DS5.10 Seguridad de la red**

Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

- **DS5.11 Intercambio de datos sensitivos**

Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

4.2.2.3.2 Administración del ambiente físico (DS12). Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera. Enfocándose en mantener la integridad, exactitud, disponibilidad y protección de los datos.

- **DS12.1 Selección y diseño del centro de datos**

Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

- **DS12.2 Medidas de seguridad física**

Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

- **DS12.3 Acceso físico**

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

- **DS12.4 Protección contra factores ambientales**

Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

- **DS12.5 Administración de instalaciones físicas**

Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

4.2.2.4 Dominio D- monitorear y evaluar (ME). Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

4.2.2.4.1 Monitorear y evaluar el control interno (ME2). Brindar transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno enfocándose en monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño.

- **ME2.1 Monitorear el marco de trabajo de control interno**

Monitorear de forma continua el ambiente de control y el marco de control de TI. Realizar la evaluación usando mejores prácticas de la industria y ría utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI.

- **ME2.2 Revisiones de auditoría**

Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

- **ME2.3 Excepciones de control**

Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones rían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas.

- **ME2.4 Control de auto evaluación**

Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

- **ME2.5 Aseguramiento del control interno**

Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoría interna o por auditores y consultores externos o por organismos de certificación. Verificar las aptitudes de los individuos que realicen la auditoria, por ej. Un Auditor de Sistemas de Información Certificado TM (CISA® por sus siglas en Inglés) debe asignarse.

- **ME2.6 Control interno para terceros**

Determinar el estado de los controles internos de cada proveedor externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede ser provisto por una auditoría externa o se puede obtener de una revisión por parte de auditoría interna y por los resultados de otras auditorias.

- **ME2.7 Acciones correctivas**

Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

4.2.3 Técnicas e instrumentos de recolección de información. Antes de empezar con el desarrollo de la auditoria, se hace indispensable conocer el diseño de los cuadros de definición de fuentes de conocimiento, en los cuales se añadirá toda la información pertinente para el desarrollo de esta auditoría, otorgada por la institución auditada. Tales como: documentación, entrevistas, manuales, archivos, políticas y normas de la entidad. Estos cuadros permiten soportar el desarrollo de este proyecto. Están compuesto por: todos los documentos y actividades necesarias, que posteriormente serán analizadas, verificadas y ejecutadas. Aunado a lo anterior se define el dominio y el proceso del COBIT al cual estará orientado el análisis de la información. Siguiendo en este orden se tienen los cuestionarios cuantitativos cuyo objeto es evaluar la situación actual del módulo de inventario del Hospital Universitario Departamental de Nariño; los cuales están compuesto por tres opciones de respuestas que son: SI, NO o NA. Paralelamente con los cuadros de fuentes conocimientos se definen el dominio y procesos del COBIT al cual hacen referencia, para conjuntamente hacer un análisis de resultados ordenado de los cuestionarios, los cuales permiten hallar el riesgo de cada proceso del Cobit. Los cuestionarios se desarrollaron otorgándoles un puntaje de 1-5 por cada pregunta, según el nivel de importancia a criterio del auditor, la suma de los puntajes de todas las preguntas da como resultado el total de la encuesta. Posteriormente se califica las columnas del SI el No y NA para tener la certeza de cuantas preguntas se respondieron por cada opción. Luego se analiza la columna de la opción NO, verificando si su resultado es alto, medio o bajo lo cual permite sacar las conclusiones del caso.

Porcentaje de Riesgo $= \frac{puntaje\ opcion\ si * 100}{Total\ encuesta - casilla\ NA}$

Luego para hallar un porcentaje de riesgo total se tiene que:

Porcentaje Riesgo total=100-**Porcentaje de riesgo**, posteriormente se tiene en cuenta los siguientes intervalos para clasificar el riesgo al cual corresponde un equis proceso del Cobit.

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 a largo plazo.

Riesgo Medio: las insuficiencias que se exhiben en este nivel son de importancia media ya que puedes 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 tomar medidas radicales e inmediatas con el objeto de reducir el riesgo, caso contrario este no permitirá alcanzar los objetivos de la entidad. Posteriormente se ilustran los cuadros de fuentes de conocimiento y cuestionarios cuantitativos desarrollados para este proyecto.

Descripción cuadros de fuentes de conocimientos.

- **ENTIDAD AUDITADA:** hace referencia al nombre de la entidad auditada.
- **AREA AUDITADA:** se refiere al área de TI, la cual será el objeto de estudio.
- **SISTEMA:** hace referencia al nombre del sistema actual de la entidad auditada.
- **RESPONSABLES:** Hace referencia a los nombres del equipo encargado de la auditoría.
- **DESCRIPCIÓN DE LA ACTIVIDAD:** se refiere a los detalles que se pretenden alcanzar en la auditoria.
- **DOMINIO:** se refiere al pilar del COBIT que será auditado.
- **PROCESO:** se refiere al proceso del COBIT que será auditado.
- **FUENTE DE CONOCIMIENTO:** se refiere a toda la documentación que da soporte a la auditoria.
- **ANALISIS:** se refiere a la verificación y comprobación de la existencia de documentos en la entidad auditada.
- **EJECUCION:** se refiere a la funcionalidad de estos documentos en la enditad.

Descripción de cuestionarios cuantitativos. Posee todos los campos anteriores, excepto fuente de conocimiento, análisis, ejecución y descripción de la actividad. Conjuntamente contienen:

- **PREGUNTA:** se refiere al listado de preguntas que serán evaluadas.
- **SI, NO Y NA:** se refiere a las opciones de respuestas.
- **TOTALES:** se refiere al puntaje del proceso del COBIT de cada uno de los campos con opción SI, NO, NA.
- **TOTAL ENCUESTA:** hace referencia a la suma de los campos de las opciones.

En las dos páginas siguientes hay un ejemplo tanto para cuestionarios cuantitativo como para fuentes de conocimiento, en este caso es para el proceso PO2. Definición de la arquitectura de información, el cual se encuentra en el dominio de Planeación y Organización.

Cuadros de definición de fuentes de conocimiento

Cuadro 1. PO2DFC.

Tipo de Registro: Definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoria.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Inventario	**SISTEMA:**	Dinámica Gerencial Hospitalaria
RESPONSABLES:	Denis Alfredo Colunge y Jorge Alexis Portilla		
DESCRIPCIÓN DE LA ACTIVIDAD: una plena y confiable satisfacción a los usuarios del sistema.			
Material de Soporte: COBIT			
DOMINIO:	Planeación y Organización (PO)	**Proceso:**	Definición de la arquitectura de información: (PO2)

Fuente de conocimiento	**Pruebas Aplicables**	
	Análisis	**Ejecución**
• Entrevistas al coordinador del área de sistemas. • Manual del módulo de inventario. • Diccionario de datos de la institución. • Entrevistas a los usuarios del módulo de inventario. • Archivo físico del contrato celebrado con **SYAC,** sobre adquisición del **DGH.**	• Analizar el manual del módulo de inventario del **DGH.** • Analizar el diccionario de datos del módulo de inventario. • Verificar cuidadosamente el contrato de adquisición de **DGH.** • Verificar la existencia de un periodo de prueba del **DGH** en el contrato de adquisición.	• Revisión rigurosa del diccionario de datos, con respecto a la base de datos funcional del **DGH.** • Obtención de datos inconsistentes. • Obtención de datos no indicados. • Comprobar falencias y detalles en la adquisición del **DGH**

Fuente: Este proyecto

Cuestionarios cuantitativos

Cuadro 2. PO2CC.

Tipo de Registro: Cuestionario Cuantitativo						
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño					
AREA AUDITADA:	Módulo de Inventario	**SISTEMA:**	Dinámica Gerencial Hospitalaria			
RESPONSABLES:	Denis Alfredo Colunge y Jorge Alexis Portilla					
Material de Soporte: COBIT						
DOMINIO:	Planeación y Organización (PO)	**Proceso:**	Definición de la arquitectura de información: (PO2)			
PREGUNTA				**SI**	**NO**	**NA**	**OBSERVACION**
1. ¿Existe un diccionario de datos en el Hospital que contenga las reglas de sintaxis del **DGH**?				4			
2. ¿Existe un manual de sistema (técnico) para el módulo de inventario del **DGH**?					4		
3. ¿Existe algún procedimiento para la clasificación de los datos sensibles y críticos de la información?				3			
4. ¿Se poseen recursos para la adquisición de nuevas tecnologías?				3			
5. ¿La información pública, confidencial y secreta se mantiene dentro de los niveles de seguridad apropiados?				4			
6. ¿Existen procedimientos para dar soporte efectivo a la administración de la información?					3		
7. ¿Todos los procesos del Hospital están sistematizados?					4		
8. ¿Están las TI y los negocios estratégicamente alineados?				4			
9. ¿los usuarios del **DGH** entiende los objetivos de TI?					3		
10. ¿Son los riesgos de TI entendidos y están siendo administrados?					3		
11. ¿La calidad del sistema de TI es apropiada para las necesidades del Hospital?					3		
12. ¿existe en el hospital archivos tanto reales como digitales, equiparables?				4			
13. ¿manejan alguna protección, sobre datos secretos, como industrial o cualquier otro?				4			
14. ¿existen documentos, con remitente, y recibido dentro de los departamentos, para generar las bases de datos?				3			
15. ¿La información del Hospital es suministrada a los usuarios, y al personal de este, es fraccionada según la importancia, entre los roles presentados?				4			
TOTALES				33	20		
				33/53	20/53		
TOTAL ENCUESTA				53			

Fuente: Este proyecto

Porcentaje de Riesgo= $\frac{33*100}{53-0}$=62.26% (Riesgo medio). Porcentaje Riesgo total=100-62.26%=37.74%(Riesgo medio).

4.2.4 Plan de pruebas. El plan de pruebas permite anotar todas las observaciones durante el proceso de la auditoria de manera secuencial, este contiene lo siguiente: prueba, proceso, tipo y acción de la prueba.

Cuadro 3. Prueba

Prueba	Proceso	Tipo	Acción
Analizar el manual del usuario del módulo de inventario	PO2	Análisis	Proporcionar una opinión a nuestro criterio de este manual.
Analizar el diccionario de datos del módulo de inventario.	PO2	Análisis	Hacer la revisión pertinente de este tipo de documento y verificar que cuente con toda la información necesaria.
Verificar como los usuarios tienen acceso al sistema.	PO2	Ejecución	Verificar que tanto los usuarios del módulo de inventario pueden hacer con el sistema, y verificar roles dentro del sistema.
Verificar el plan tecnológico de arquitectura de sistemas	PO3	Análisis	Verificar que en la entidad se están manejando una sola línea de tecnología tanto software como Hardware. Con el objeto de que no hayan incompatibilidades que disminuyen el rendimiento de los mismos.
Analizar el plan de desarrollo respecto al ambiente y todo lo que rodea a la institución	PO3	análisis	Verificar que se tiene una plena identificación de los posibles y diferentes sucesos que le rodea a la entidad.
Verificar que el personal de la entidad está capacitado para el manejo del **DGH**.	PO7	Ejecución	Realizar entrevistas prácticas para la observación de la pericia de los usuarios del sistema.
Verificar que los usuarios cumplen la política del buen uso de los equipos	PO9	Ejecución	Verificar que cada usuario tenga su propia contraseña. Y la pericia en el manejo de los equipos y del módulo.
Verificar si la institución cuenta con un plan de mitigación de riesgos.	PO9	Análisis	Comprobar que este plan se está ejecutando en todas las áreas donde manipule el sistema de información.
Verificar que los pedidos de las áreas se estén realizando por medio del sistema.	AI3	Ejecución	Verificar que los pedidos a los almacenes se lleven de manera sistematizada. Para evitar malos entendidos tanto actuales como futuros.
Verificar la metodología de pruebas, al momento de implantar nuevos aplicativos.	AI7	Análisis	Revisar que exista un documento que sea capaz de soportar el proceso de monte y desmonte de un sistema. Aunado a lo anterior que contenga todo el algoritmo de funcionamiento técnico; una vez puesto en marcha
Verificar que después de la implantación de un nuevo sistema, se realice una previa capacitación del personal.	AI7	Ejecución	Entrevistar al personal e indagarlo respecto a lo que puede y sabe hacer con el sistema.
Verificar que se están elaborando los BACKUP en la entidad.	DS5	Análisis	Comprobar que los BACKUP se están elaborando de manera frecuente en el día.
Verificar los roles de acceso al sistema.	DS5	Ejecución	Comprobar que los usuarios solo puedan hacer lo que el administrador del sistema le permitió.
Verificar que los servidores estén físicamente seguros	DS5	Análisis	Determinar y realizar recomendaciones respecto a los sitios adecuados para el alojamiento de servidores.
Verificar que las contraseñas se cambian periódicamente.	DS5	Ejecución	Revisar que se cumpla con las políticas establecidas en el programa establecido por la institución.
Verificar que la trazabilidad de la información es rigurosa.	DS5	Ejecución	Comprobar que la información que se le suministra al sistema es coherente con la información arrojada por el sistema.
Verificar la seguridad de la red	DS5	Ejecución	Comprobar las fortalezas o vulnerabilidades que se encuentran expuesto los servidores del Hospital
Verificar los reportes de falla existentes en el **DGH**	DS12	Análisis	Comprobar que las fallas ya han sido enviadas al proveedor, y éste a su vez les haya proporcionado una solución adecuada.
Verificar la eficiencia de la central eléctrica.	DS12	Análisis	Comprobar que la central eléctrica de la institución es suficiente, para abastecer las necesidades primordiales de la entidad.
Verificar que se está realizando la monitorización de TI en la institución, teles como: sistemas, redes, etc.	ME2	Ejecución	Comprobar con un software la adecuada seguridad de la red, entre otros.

Fuente: Este proyecto

4.2.5 Matriz de probabilidad e impacto. Según el MECI este componente es primordial en el desarrollo de la auditoria ya que permite determinar el nivel de riesgo de cada uno de los hallazgos encontrados, tanto cualitativa como cuantitativamente. Por medio de esta clasificación se puede observar cuál de los riegos es catastrófico, importante, moderado o aceptable y a su vez el respectivo valor del riesgo.

Cuadro 4. Matriz

Probabilidad				
	Alto(3)	**Riesgo Moderado (15)**	**Riesgo Importante (30)**	**Riesgo Inaceptable (60)**
	Medio(2)	**Riesgo Tolerable (10)**	**Riesgo Moderado (20)**	**Riesgo Importante (40)**
	Bajo(1)	**Riesgo Aceptable (5)**	**Riesgo Tolerable (10)**	**Riesgo Moderado (20)**
		Bajo(leve)(5)	**Medio(moderado)(10)**	**Alto(catastrófico)(20)**
			Impacto	

Fuente: Este proyecto

4.2.5.1 Descripción del formato de hallazgos

- **ENTIDAD AUDITADA:** hace referencia al nombre de la entidad auditada.
- **REF:** cuestionario que determino el Hallazgo.
- **AREA AUDITADA:** se refiere al área de TI la cual será el objeto de estudio.
- **SISTEMA:** hace referencia al nombre del sistema actual de la entidad auditada.
- **RESPONSABLES:** hace referencia a los nombres del equipo encargado de la auditoría.
- **Probabilidad:** hace referencia a la posibilidad de ocurrencia del riesgo.
- **Impacto:** hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- **Descripción Hallazgo:** se refiere a los detalles del hallazgo.
- **NIVEL DE RIESGO:** hace referencia al valor cualitativo o cuantitativo del riesgo.
- **CONSECUENCIA:** se refiere al efecto actual o futuro, que tendrá la organización, de no tomar las precauciones oportunas.
- **RECOMENDACIONES:** hace referencia a las descripciones correctivas de carácter preventivo.

En la siguiente página se encuentra el formato de hallazgos.

Cuadro 5. Hallazgos

	Hallazgos	**Ref. Plan**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definición de la arquitectura de información: (PO2)
Descripción Hallazgo:			
Probabilidad : **Impacto:**			
Nivel de Riesgo:			
Consecuencia:			
Recomendaciones:			

Fuente: Este proyecto

Cuadro 6. Hallazgo 1

	Hallazgos	**Ref. Plan PO2_01**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definición de la arquitectura de información: (PO2)
Descripción Hallazgo:			
• No existe un manual de sistema técnico. • No existen procedimientos para dar soporte efectivo a la administración de la información. • No existe una sistematización total de los procesos en el hospital. • La calidad de TI en su totalidad no es apropiada para la entidad.			
Probabilidad : Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La ausencia de un manual de sistema técnico ocasiona un deficiente soporte a la hora de administrar cambios, en el DGH.net. • La ausencia de procedimientos de soportes generan dificultad en los procesos vuelta tras. • La ausencia de sistematización de procesos en el hospital es causante de exceso de papel. Aunado a lo anterior implica un problema de carácter ambiental. • La ausencia de calidad de TI hace que los recursos tanto Hardware como software no se aprovechen a su máximo rendimiento.			
Recomendaciones:			
• En las próximas adquisiciones tecnológicas del HUDN se recomienda que en el contrato con SYAC se establezca la entrega del manual de sistema técnico, donde se especifiquen con lujos y detalles todas las características técnicas del software. • Documentar todos y cada uno de los procesos que se lleven a cabo en la administración de la información. • Realizar una sistematización de casi todos los procesos, salvo aquellos que realmente no se puedan sistematizar. • Utilizar un solo tipo de tecnología, con el objeto de evitar incompatibilidades que disminuyan el rendimiento de estas.			

Fuente: Este proyecto

Cuadro 7. Hallazgo 2

	Hallazgos	**Ref. Plan PO3_02**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Determinar la Dirección Tecnológica: (PO3)
Descripción Hallazgo:			
• No existen técnicas de migración de datos. • No existe un área de sistemas segura. • No existe un comité técnico de sistemas.			
Probabilidad: Alta **Impacto:** catastrófico			
Nivel de Riesgo: Inaceptable (60)			
Consecuencia:			
• La ausencia de estrategias de migración de datos en el hospital es grave, debido a que se hace pero no se lleva una bitácora de la metodología empleada para este proceso lo cual crea indispensabilidad de puestos en la organización. • La ausencia de un área de sistemas segura en el Hospital es grave, porque la información es uno de los activo más importante dentro una organización, de tal manera que esta entidad no debería correr con este riesgo, de ocurrir un siniestro quedarían literalmente en el aire. • La ausencia de un comité técnico de sistemas, es enorme porque este permite asesorar y documentar todos los procesos realizados en el área de sistemas.			
Recomendaciones:			
• Documentar todo el proceso de migración de datos, para que con facilidad otros peritos no tengan ningún inconveniente al momento de realizar este proceso. • Implementar un proyecto de construcción de un área de sistemas segura, en la cual solo el personal autorizado tenga acceso a la información. No como la actual que cualquiera puede tener acceso si así lo decide. • Crear un comité técnico de sistemas que en el recaiga toda la responsabilidad de asesoría y documentación de los procesos del área de sistemas.			

Fuente: Este proyecto

Cuadro 8. Hallazgo 3

	Hallazgos	**Ref. Plan PO7_02**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Administrar Recursos Humanos de TI: (PO7)
Descripción Hallazgo:			
• No existe una verificación periódica del personal en sus funciones. • No existen programas de calificación y certificación de los usuarios del DGH.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La ausencia de este proceso en el Hospital hace que el personal realiza sus actividades a su manera. • La ausencia de este proceso en la entidad implica que no capten de manera adecuada los procesos en los cuales será su desempeño.			
Recomendaciones:			
• Realizar verificaciones periódicas al personal, respecto a su desempeño en las funciones y como está elaborando los procesos. • Implementar programas de calificación y certificación de los usuarios del DGH, y un entrenamiento periódico del personal.			

Fuente: Este proyecto

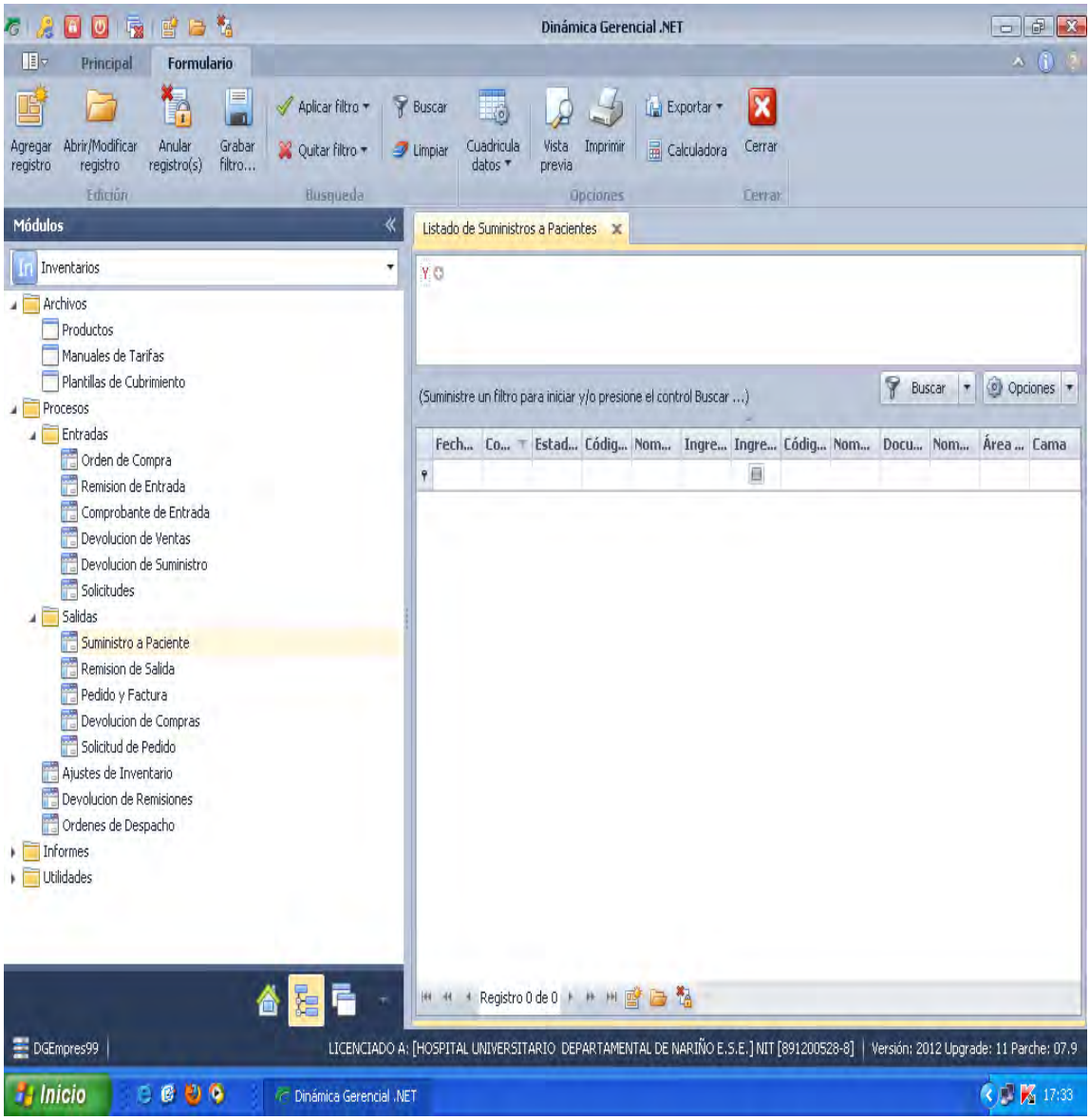
Cuadro 9. Hallazgo 4

	Hallazgos	**Ref. Plan PO7_03**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Administrar Recursos Humanos de TI: (PO7)
Descripción Hallazgo:			
• No existe una asignación de roles rigurosa.			
Probabilidad: Alta **Impacto:** Catastrófico			
Nivel de Riesgo: Inaceptable (60)			
Consecuencia:			
• La ausencia rigurosa de asignación de roles en el DGH conlleva a posibles errores con o sin intensión en la administración de las entradas de información al sistema.			
Recomendaciones:			
• Otorgar roles serios a los usuarios del DGH en el módulo de inventario, es decir que solo se les debe habilitar del sistema lo que necesite el usuario para el desarrollo de sus actividades propuestas por el jefe. No como en la actualidad, algunos usuarios no hacen uso de otro segmento del sistema por solo respeto e intuición de que puede estar mal el uso no autorizado de un rol que no les compete.			

Fuente: Este proyecto

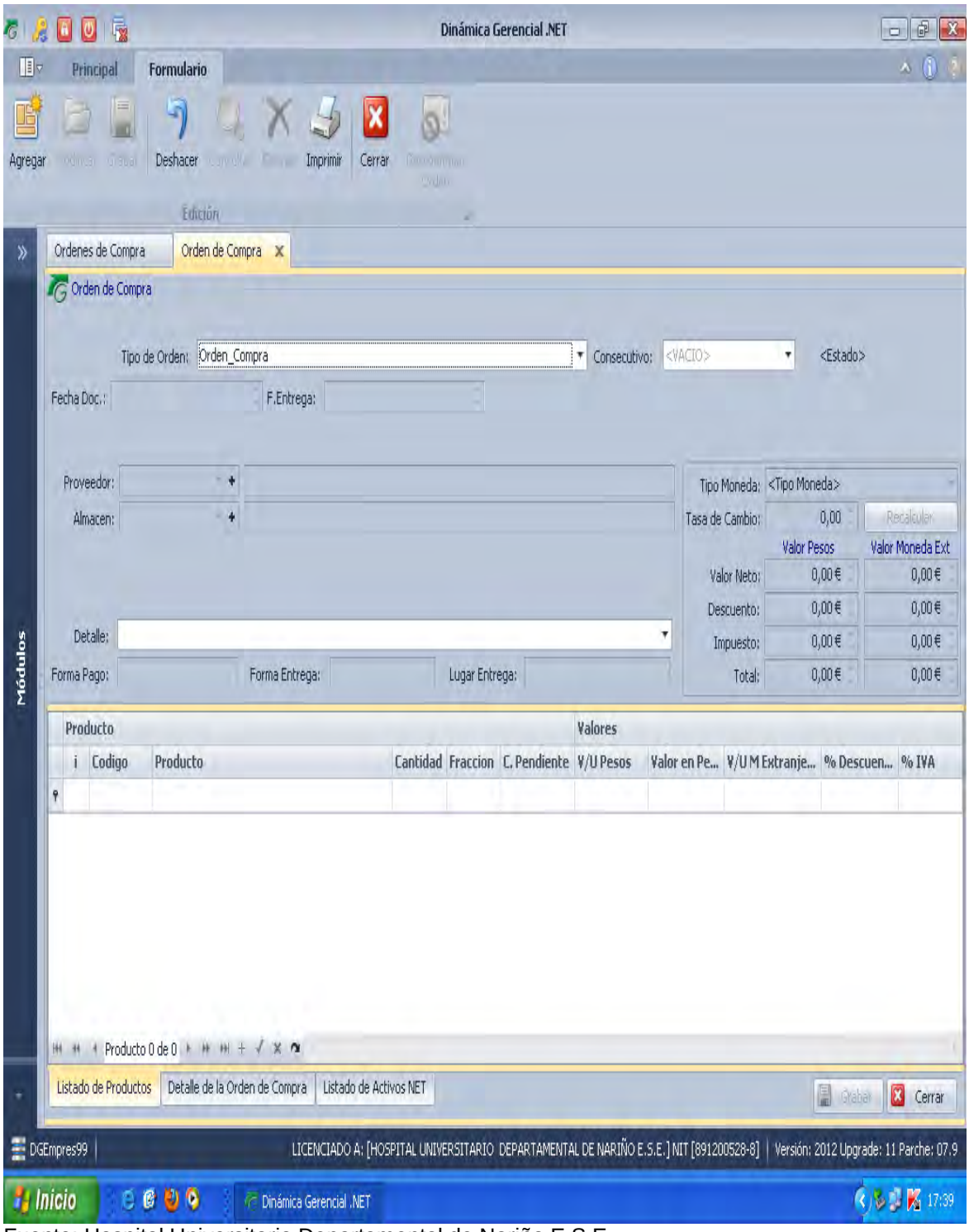
Para más certificación acerca de los roles de entradas de información al módulo de inventario, se tomaron pantallazos al DGH.net tanto en RECURSOS FARMACÉUTICOS como en ALMACÉN. Como se puede observar en las siguientes figuras, no se tienen limitaciones rigurosas en el sistema, los usuarios de RECURSOS FARMACÉUTICOS pueden hacer órdenes de compra y comprobantes de entradas cosas que a ellos no les compete, le compete a almacén. Y a su vez los de ALMACÉN también tienen habilitado roles que no utilizan en su quehacer diario.

Figura 10. Recursos_farmaceuticos_PO7_03



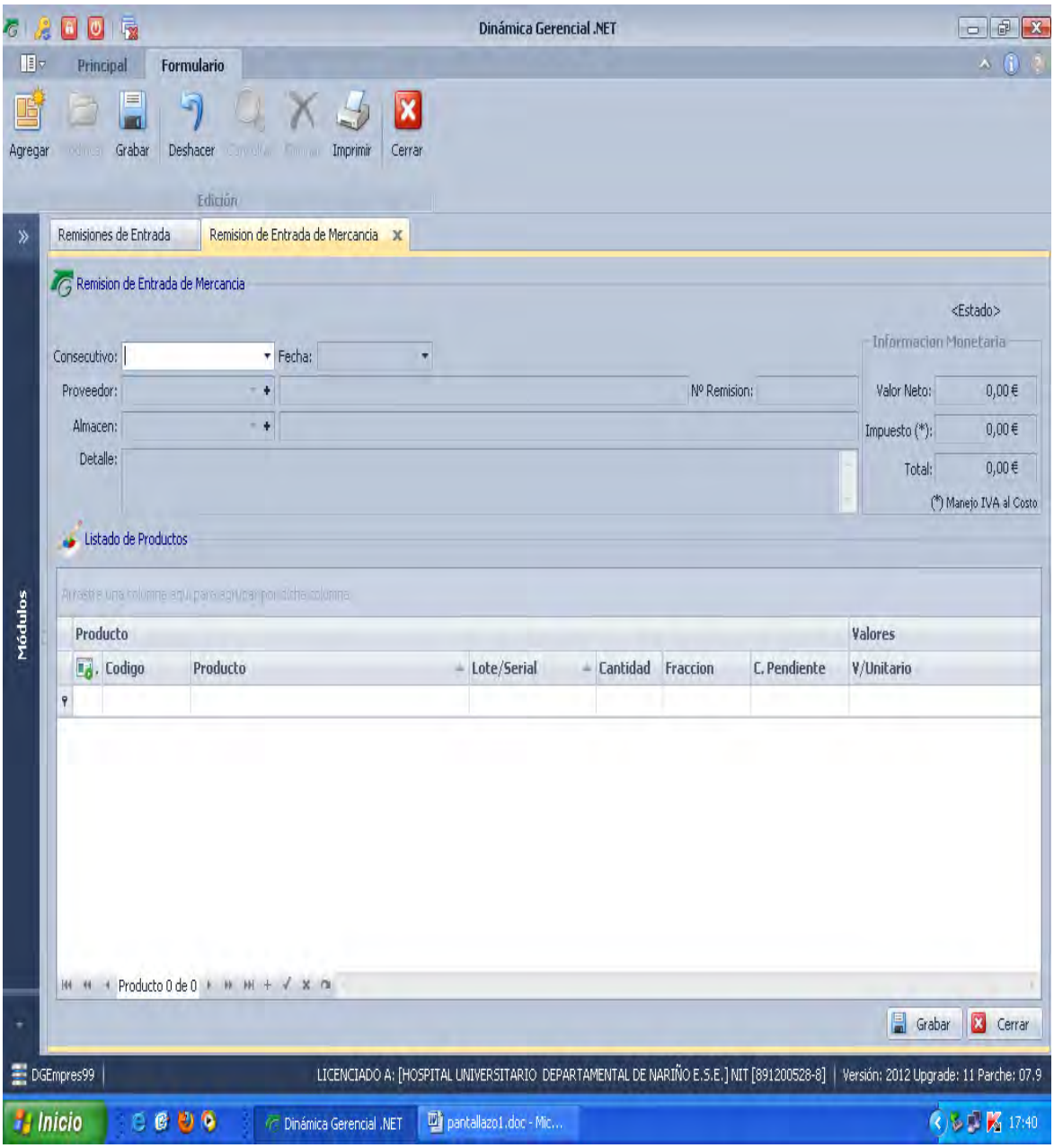
Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 11. Recursos Farmacéuticos PO7_03



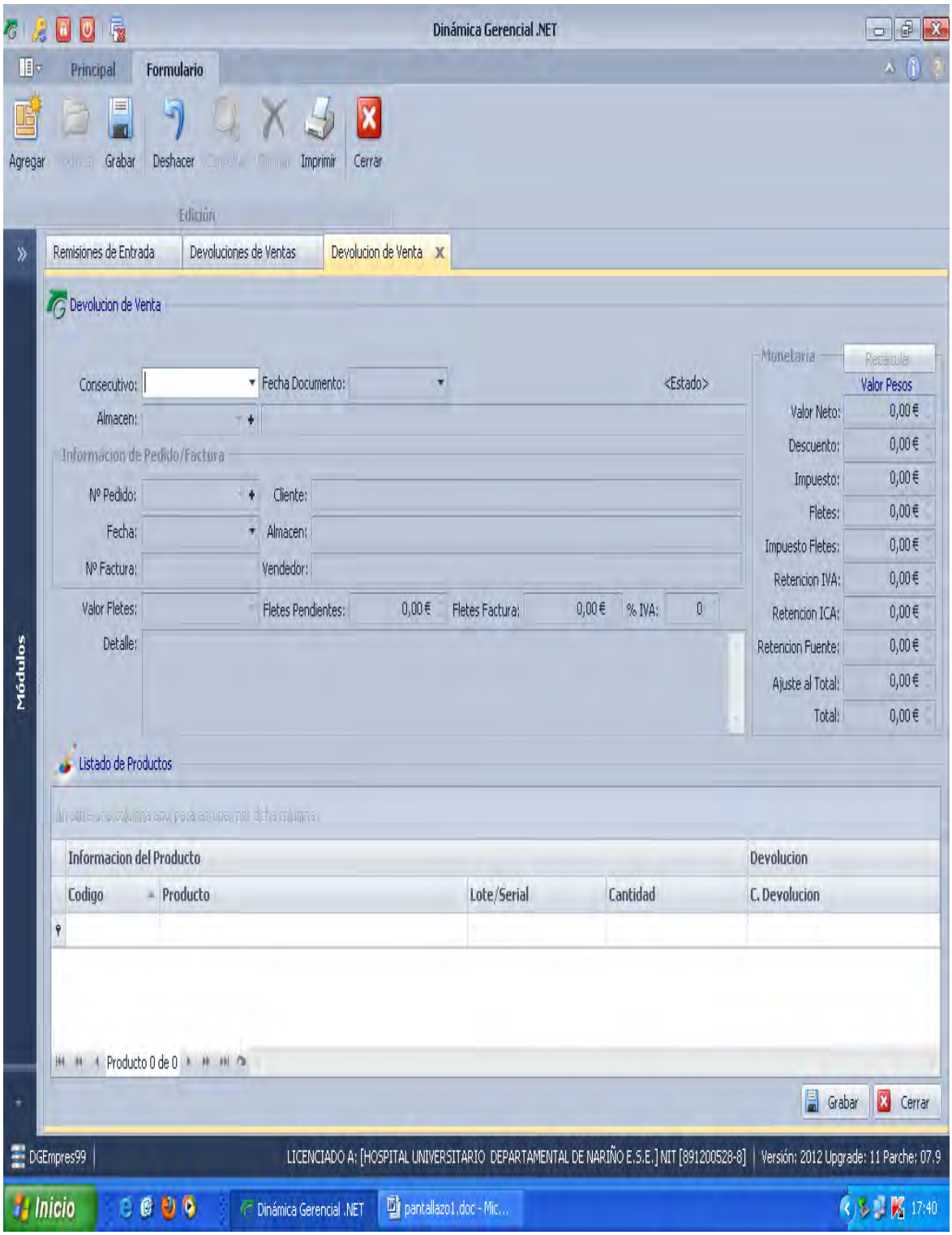
Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 12. Recursos farmacéuticos PO7_03



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

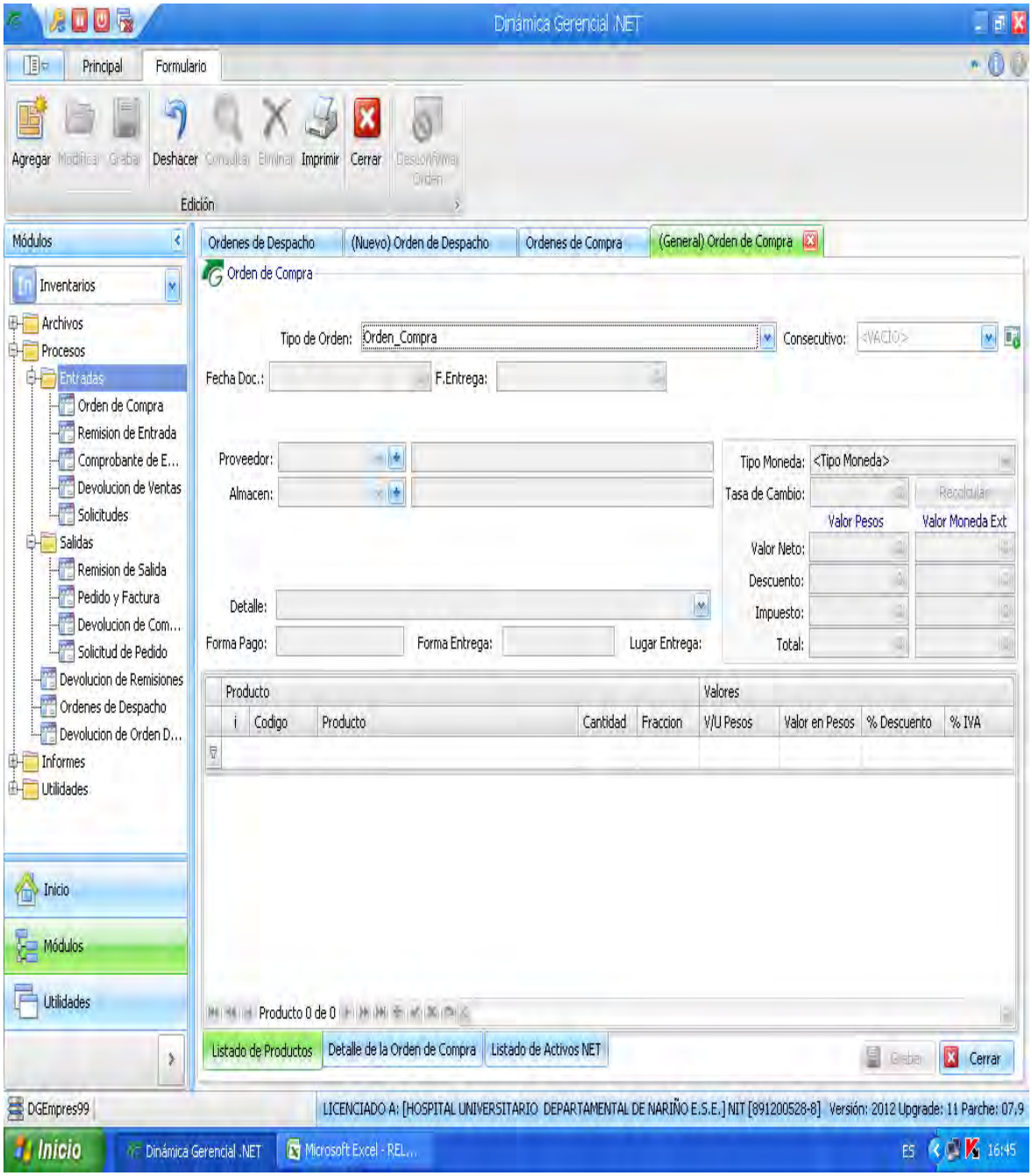
Figura 13. Recursos farmacéuticos PO7_03



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

A su vez el administrador del almacén tiene habilitado gran parte del módulo de inventario que no utiliza.

Figura 14. Almacén PO7_03



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Cuadro 10. Hallazgo 5

	Hallazgos	**Ref. Plan PO7_08**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Administrar Recursos Humanos de TI: (PO7)
Descripción Hallazgo:			
• No existe un documento de garantía, que exprese que el personal del Hospital y específicamente los que trabajan en el DGH coadyuven a mitigar riesgos de este.			
Probabilidad: Alta **Impacto:** Leve			
Nivel de Riesgo: Moderado (15)			
Consecuencia:			
• La ausencia de mitigación de riesgos sin documento de garantía en la entidad con respecto al personal, implica que los procesos que los usuarios están realizando se efectúan sin calidad certificada.			
Recomendaciones:			
• Hacer la transferencia del conocimiento, reasignar responsabilidades y eliminar los privilegios de accesos a la información, de esta manera se elimina la dependencia y riesgos actuales, presentes y futuros.			

Fuente: Este proyecto

Cuadro 11. Hallazgo 6

	Hallazgos	**Ref. Plan PO9_06**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Evaluar y Administrar los Riesgos de TI: (PO9)
Descripción Hallazgo:			
• No existe un plan de recuperación y minimización del impacto en los procesos del Hospital que garanticen la continuidad del funcionamiento del Módulo de Inventario del DGH. • • El Hospital no cuenta un plan de mitigación de riesgos del Sistema de Información DGH. • No existe un procedimiento que en el cual se verifique que la construcción, prueba e implantación de los controles y procedimientos de seguridad sean formalmente aprobados antes de que se utilice el sistema información **DGH.**			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La ausencia de un plan documentado de recuperación tanto del módulo de inventario como del DGH implican en la dependencia del personal a cargo de esta actividad, la cual se está realizando sin soporte. • • La ausencia de un plan de mitigación de riesgos implica que no se tiene la claridad de magnitud de los impactos en caso de un eventual siniestro.			
Recomendaciones:			
• Implementar un repositorio digital donde se almacenen todos los documentos pertinentes de los procesos manejados en el área de sistemas. • • Realizar un plan de mitigación de riesgos donde se especifique todos y cada uno de los sectores del HUDN que están propensos a un eventual siniestro, y evaluar el impacto que causaría en caso de ocurrir. Se recomienda que al momento de establecer el contrato con SYAC que les faciliten todas las pruebas realizadas a este software.			

Fuente: Este proyecto

Cuadro 12. Hallazgo 7

	Hallazgos	**Ref. Plan AI3_03**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Adquirir e Implementar(AI)	**Proceso:**	Adquirir y Mantener Infraestructura Tecnológica: (AI3)
Descripción Hallazgo:			
✓ El hospital no cuenta con un plan de mantenimiento de la infraestructura tecnológica que garantice que se están controlando los cambios tecnológicos.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
✓ La ausencia de un plan de mantenimiento documentado implica en que no se tiene una claridad de las fechas de revisiones a toda la infraestructura tecnológica.			
Recomendaciones:			
✓ Crear un plan de mantenimiento que permita tener la certeza y rigor de las actividades de mantenimiento. Además que se estén efectuando en el tiempo oportuno e indicado, y a su vez una correcta documentación de todas las incompatibilidades encontradas y las correcciones de las mismas.			

Fuente: Este proyecto

Cuadro 13. Hallazgo 8

	Hallazgos	**Ref. Plan AI3_02**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Adquirir e Implementar(AI)	**Proceso:**	Adquirir y Mantener Infraestructura Tecnológica: (AI3)
Descripción Hallazgo:			
✓ El área de sistemas del Hospital no se encuentra en la capacidad, de estar a la vanguardia de optimizar el sistema, de manera productiva y segura. ✓ No existe una adecuada seguridad, integridad, y disponibilidad, de la infraestructura TI en el Hospital			
Probabilidad: Media **Impacto:** Moderado			
Nivel de Riesgo: Moderado (20)			
Consecuencia:			
✓ No estar a la vanguardia implica que el crecimiento de la entidad va ser inseguro, ya que se está omitiendo la documentación de muchos procesos fundamentales. ✓ No tener en la entidad una seguridad, integridad, y disponibilidad adecuada implica que los procesos se realizan de manera lenta lo cual se pierde mucho tiempo, en reinicio de los equipos, cuando el sistema no responde debido a la cantidad de usuarios al tiempo ingresando información. Además La red de la entidad cuenta con distintos tipos de cableado lo cual es un factor de disminución de rendimiento en la tecnología utilizada. Por otro lado el riesgo que se corre si algún usuario del sistema le da por hacer pruebas e ingresar valores en las opciones que tiene habilitadas.			
Recomendaciones:			
✓ Empezar por documentar todos los procesos que se hagan respecto a infraestructura tecnológica, los parches que se le hagan al sistema, las auditorías internas con claridad y autonomía en sus reportes, administrar de manera rigurosa los roles del sistema, entre otros. ✓ Empezar por conseguir seguridad, integridad, y disponibilidad adecuada, corrigiendo todas y cada una de las faltas que posee la infraestructura de la entidad teles como: ✓ La red de la entidad cuenta con distintos tipos de tecnología como: cableado, switches, etc. lo cual es un factor de disminución de rendimiento en la tecnología utilizada. ✓ El riesgo que se corre si algún usuario del sistema le da por hacer pruebas e ingresar valores en las opciones que tiene habilitadas. ✓ Establecer cámaras en lugares estratégicos. Es decir en la parte donde está el servidor principal, además de estar al lado de la central eléctrica.			

Fuente: Este proyecto

Cuadro 14. Hallazgo 9

	Hallazgos	**Ref. Plan AI7_06**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Adquirir e Implementar(AI)	**Proceso:**	Instalar y Acreditar Soluciones y Cambios: (AI7)
Descripción Hallazgo:			
• Cuándo se está implantando un nuevo sistema en el Hospital, o se está modificando un sistema ya existente, no se cuenta con un plan para la implantación de este, y un plan de respaldo vuelta atrás.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La ausencia de un plan documentado para implantación y un plan de respaldo vuelta a tras implica en que no se tendría la claridad de cada uno de los procesos en futuras instalaciones del sistema, y mucho menos saber dónde ocurrieron errores durante el proceso. Por otro lado si la transición no es exitosa volver al anterior software será muy tedioso y complicado, ya que no existe ningún documento de la instalación y administración de este software.			
Recomendaciones:			
• Crear un plan documentado para la implantación y plan de respaldo vuelta atrás de los sistemas de la entidad. El plan debe definir claramente el diseño de versiones, construcción de paquetes de versiones, procedimientos de implantación e instalación, manejo de incidentes, controles de distribución, almacenamiento de software, revisión de la versión y documentación de cambios.			

Fuente: Este proyecto

Cuadro 15. Hallazgo 10

	Hallazgos	**Ref. Plan AI7_08**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Adquirir e Implementar(AI)	**Proceso:**	Instalar y Acreditar Soluciones y Cambios: (AI7)
Descripción Hallazgo:			
• No existe una evaluación de las pruebas practicadas a los sistemas por parte de la gerencia del Hospital.			
Probabilidad: Alta **Impacto:** Leve			
Nivel de Riesgo: Moderado (15)			
Consecuencia:			
• La ausencia de una evaluación de las pruebas practicadas a los sistemas por parte de la gerencia del Hospital implica en el desinterés de la unión entre paciente-información. Se sabe que el paciente es lo más importante en este hospital, pero la información también debe serlo, es decir deben ir de la mano; sin un buen sistema de información una organización considerable en tamaño, personal e infraestructura no es exitosa.			
Recomendaciones:			
• La gerencia debe solicitar que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año. La gerencia debe estar involucrada en el proceso de adquisición de los sistemas, no solo gerencia de información. Esto le permitirá a gerencia garantizar que los procesos con los cuales está funcionando la empresa están a acorde con los estándares de calidad perseguidos por el hospital.			

Fuente: Este proyecto

Cuadro 16. Hallazgo 11

	Hallazgos	**Ref. Plan AI7_09**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Adquirir e Implementar (AI)	**Proceso:**	Instalar y Acreditar Soluciones y Cambios:(AI7)
Descripción Hallazgo:			
• No se realizan revisiones al sistema de información luego de la implantación o modificación del sistema actual.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La omisión de revisiones en el sistema de información implica en no tener claridad ante fallos del sistema.			
Recomendaciones:			
• Realizar revisiones periódicas al sistema, lo cual permitirá hallar los errores que se puedan presentar en la ejecución del sistema montado.			

Fuente: Este proyecto

Cuadro 17. Hallazgo 12

	Hallazgos	**Ref. Plan DS5_02**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Entregar y Dar Soporte(DS)	**Proceso:**	Garantizar la Seguridad de los Sistemas: (DS5)
Descripción Hallazgo:			
• Los servidores no están asegurados físicamente • Las contraseñas no se cambian periódicamente de acuerdo al programa establecido			
Probabilidad: Alta **Impacto:** catastrófico			
Nivel de Riesgo: Inaceptable (60)			
Consecuencia:			
• La ausencia de seguridad en los servidores puede ser fatal para la organización, ya que corren el riesgo de ser dañados, robados e incendiados por terceros. • El no cambiar las contraseñas sé corre el riesgo de que alguien pueda ingresar a las diferentes cuentas de los usuarios del DGH y dañar la información.			
Recomendaciones:			
• Crear lo antes posibles un área segura para posesionar los servidores de la entidad. • Realizar un cambio periódico de las contraseñas en la entidad, para evitar sabotajes cibernéticos, y concientizar a los usuarios de que la clave de acceso no prestar. Respecto al acceso al servidor principal de la entidad encriptar la clave y cerrar puertos en lo más que se pueda.			

Fuente: Este proyecto

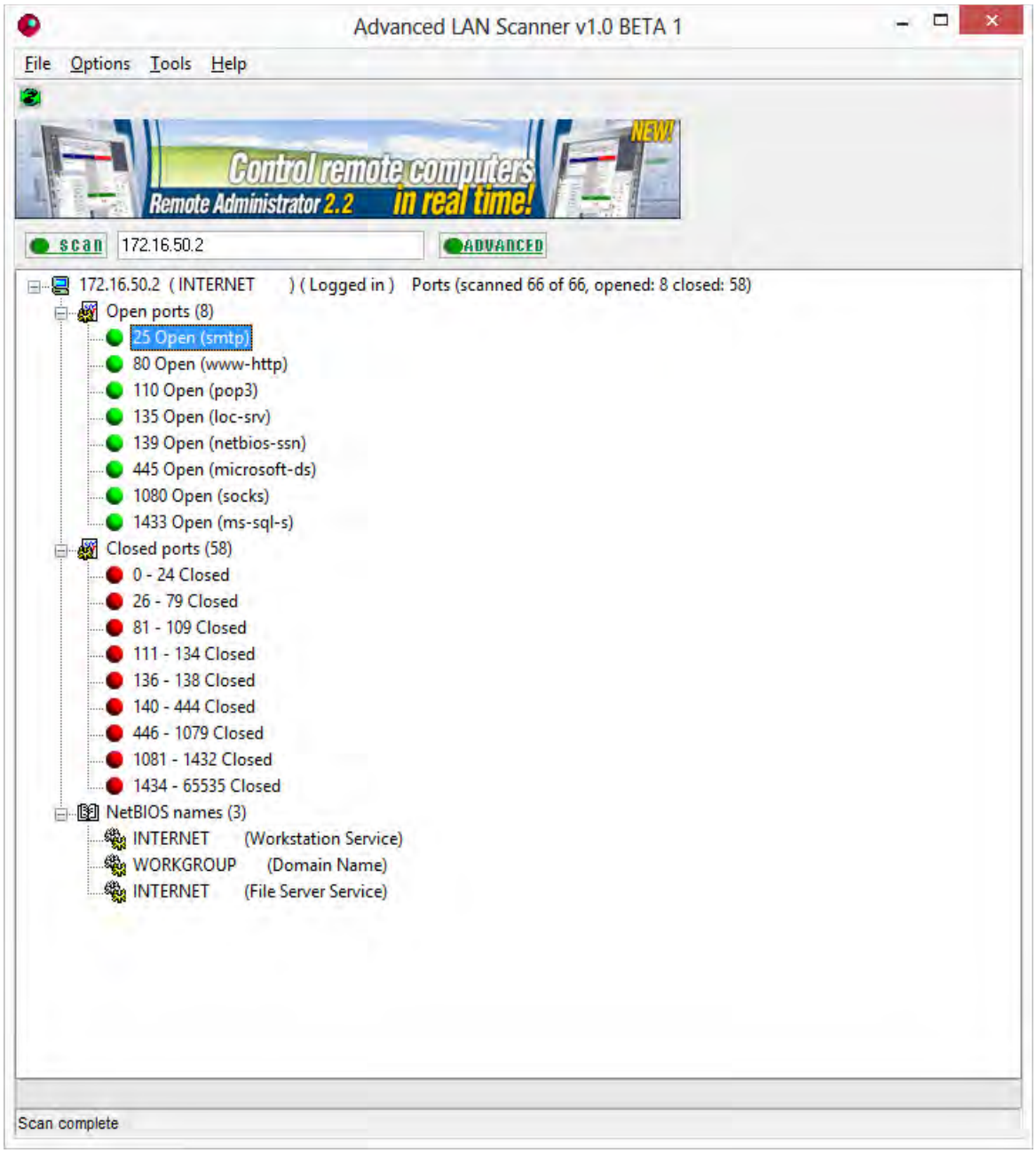
Cuadro 18. Hallazgo 13

	Hallazgos	**Ref. Plan DS5_10**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Entregar y Dar Soporte(DS)	**Proceso:**	Garantizar la Seguridad de los Sistemas: (DS5)
Descripción Hallazgo:			
• No es observada a plenitud la seguridad de archivos y de la base de datos. • No se garantiza que se utilicen técnicas de seguridad y procedimientos de seguridad asociados para autorizar accesos y controlar los flujos de información desde y hacia la red.			
Probabilidad: Alta **Impacto:** catastrófico			
Nivel de Riesgo: Inaceptable (60)			
Consecuencia:			
• La ausencia de certeza de seguridad en los datos en una organización, ocasiona incertidumbre en su misión y visión. • La ausencia de verdaderas técnicas de seguridad con respecto a intrusiones desde internet en el hospital son graves, ya que provocaría un holocausto en uno de los activos más importantes de una entidad.			
Recomendaciones:			
• Crear controles de seguridad de manera inmediata en los servidores, y especialmente en el servidor principal donde se encuentra la base de datos de la organización, la cual contiene toda la información de la entidad. Deben tener en cuenta el almacenamiento en la nube. No deben tener acceso a la DB tantos peritos; documentar los proceso que lleve la persona que esté a cargo para no crear dependencias de este. • Implementar técnicas y metodologías de seguridad en la red para proteger la información de manera adecuada y segura tales como: pasar todos los servidores a ambiente Linux, al menos el principal. Por otro lado contar con software de detección de instrucciones, firewalls y segmentación de la red.			

Fuente: Este proyecto

Para más certificación acerca de la ausencia de técnicas de seguridad, se evaluó la seguridad de los puertos de la red con un software (ADVANCED LAN Scanner), y se encontró que: el SERVIDOR DE INTERNET con IP LOCAL (PROXY). Poseía los siguientes puertos abiertos, los cuales se muestran en la siguiente imagen. Además está bajo Windows.

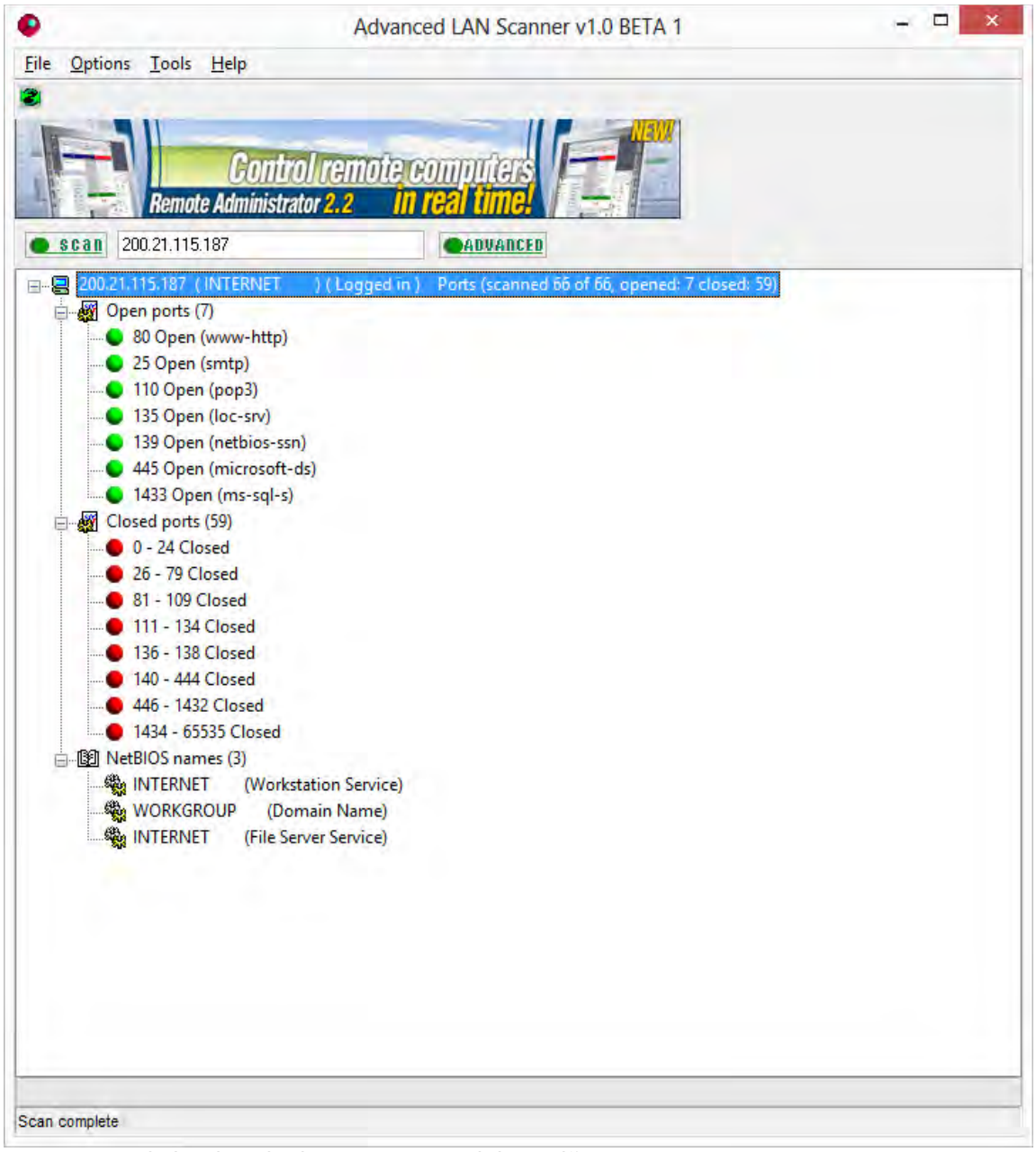
Figura 15. DS5_10



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Con respecto al SERVIDOR DE INTERNET IP PUBLICA con acceso a internet, además administra el correo institucional. Es por este servidor o por el de la anterior imagen, que pueden atacar cibernéticamente a toda la información que cuenta el Hospital, almacenada en el servidor principal de datos. Este servidor está bajo Windows. El cual posee un gran número de puertos abiertos.

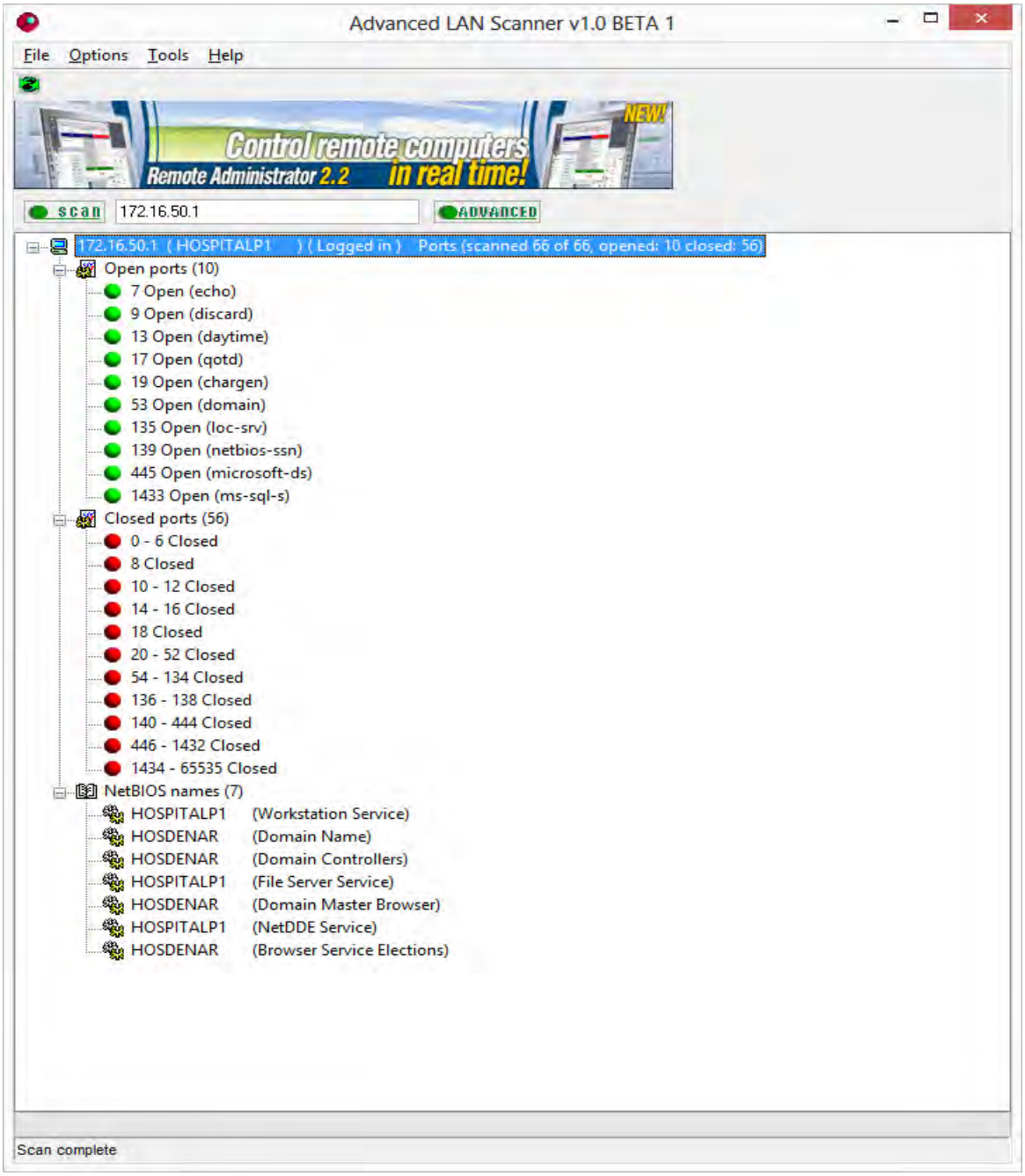
Figura 16. DS5_10



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

El SERVIDOR PRINCIPAL DE DATOS, es el que cuanta con toda la información del Hospital Universitario Departamental de Nariño. Esta bajo Windows. Posee un gran número de puertos abiertos.

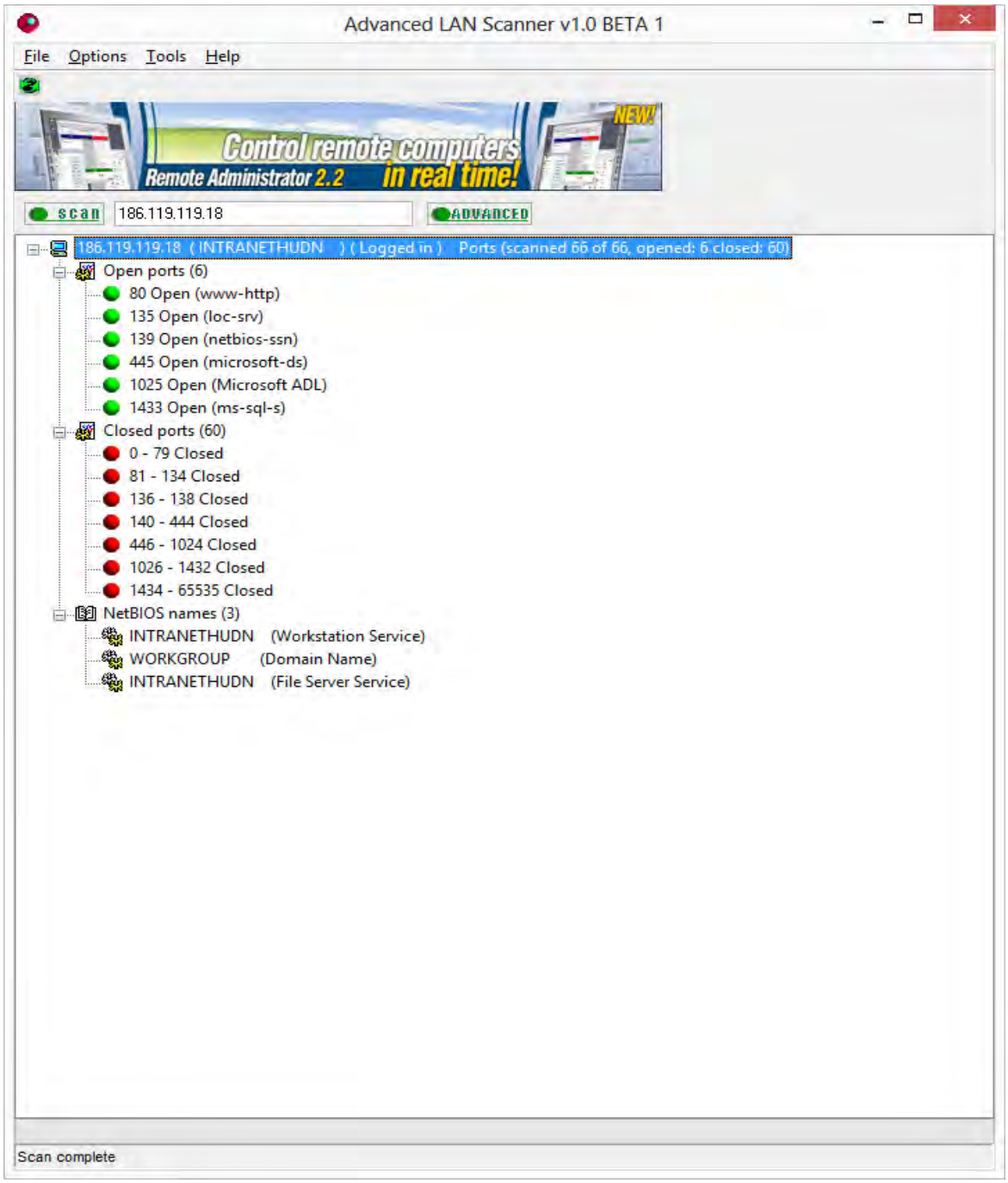
Figura 17. DS5_10



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

INTRANET CORPORATIVA (ACCESO A INTERNET), es el encargado de la intranet, también se encuentra bajo Windows, se observa que tiene un gran número de puertos abiertos.

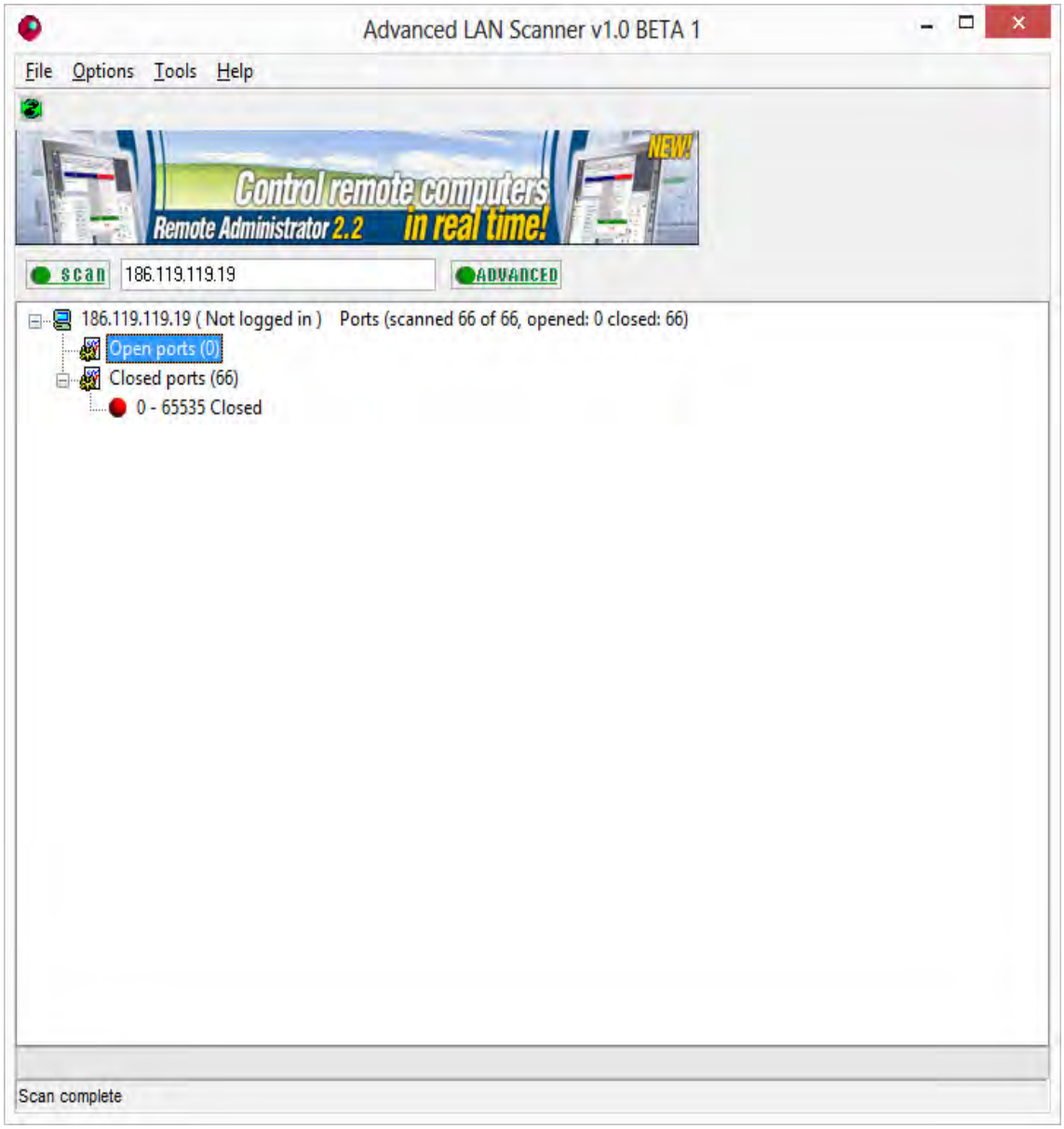
Figura 18. DS5_10



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

SERVIDOR INTERNET FIREWALL (SERVIDOR INTERNET). Este servidor es el que tiene la mayor seguridad de la institución. Ya que está bajo Linux. Realizar una migración de estos servidores a Linux. Al menos los más importantes que determine el área de sistemas. Por otro lado si se observa la **Figura 19. Imagen10_ DS5_10,** la cual hace referencia a un y único servidor bajo Linux en el hospital, se ve el poderío de Linux en cuanto a seguridad, no existe ningún puerto abierto propenso a un ataque cibernético.

Figura 19. DS5_10



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Cuadro 19. Hallazgo 14

	Hallazgos	**Ref. Plan DS12_01**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Entregar y Dar Soporte(DS)	**Proceso:**	Administración del Ambiente Físico: (DS12)
Descripción Hallazgo:			
• No se definieron ni diseñaron centros de datos para el equipo de TI ni se tuvieron en cuenta las normas de seguridad física y las leyes de seguridad física en el trabajo.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• Por la omisión del hallazgo anterior, la E.S.E puede correr graves riesgos, ya que en el HUDN no se le presta atención a estas anomalías. Ejemplo el centro de datos está al lado de la central eléctrica, en caso de incendio habría graves consecuencias; no solo víctimas humanas o pérdidas materiales, si no la pérdida de la información de la institución.			
Recomendaciones:			
• Rediseñar un centro de datos y tener en cuenta todos los factores de riesgos que incurriría la organización. Se recomienda que exista un complemento paciente-información. Que no solo la prioridad sea el paciente sino también la información.			

Fuente: Este proyecto

Cuadro 20. Hallazgo 15

	Hallazgos	**Ref. Plan ME2_02**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Monitorear y Evaluar(ME)	**Proceso:**	Monitorear y Evaluar el Control Interno: (ME2)
Descripción Hallazgo:			
• No se monitorea la eficiencia y eficacia de la auditoría interna.			
Probabilidad: Alta **Impacto:** leve			
Nivel de Riesgo: Moderado (15)			
Consecuencia:			
• La omisión de monitoreo de la auditoría interna permite concluir que los procesos en el hospital no están siendo plenamente identificados y documentados. Aunado a lo anterior no existe una certificación de que los resultados de estas auditorías son correctas y eficientes.			
Recomendaciones:			
• Monitorear la eficiencia de estas auditorías y permitir mostrar y documentar todas las anomalías encontradas en estas.			

Fuente: Este proyecto

Cuadro 21. Hallazgo 16

	Hallazgos	**Ref. Plan ME2_03**	
Entidad Auditada:	Hospital Universitario Departamental de Nariño		
Sistemas:	DGH.net	**Área Auditada:**	Módulo de Inventario
Responsables: Denis Colunge Y Jorge Portilla			
Material de Soporte: COBIT			
Dominio:	Monitorear y Evaluar(ME)	**Proceso:**	Monitorear y Evaluar el Control Interno: (ME2)
Descripción Hallazgo:			
• No existe una identificación de las excepciones de control, ni se identifican sus causantes, ni se reportan a los interesados. • No existe la evaluación de control interno por parte de terceros.			
Probabilidad: Alta **Impacto:** Moderado			
Nivel de Riesgo: Importante (30)			
Consecuencia:			
• La ausencia de identificación, causantes y reportes de las excepciones de control en la entidad implica en que muchos procesos en la organización pueden estar funcionando de manera inadecuada. Y no se hace nada para corregirlos ya que las anomalías encontradas se omiten. • La omisión de auditorías externas en el hospital implica en que no se les inspeccione completamente. Es decir desde fuera se observa mejor, además se pueden hacer con autonomía todos y cada uno de los reportes del caso.			
Recomendaciones:			
• Reportar tanto al jefe de área como a gerencia de todas las anomalías encontradas en la auditoría interna, para que se tomen todas las correcciones del caso y así cumplir con la misión y visión de la entidad. • • Realizar evaluaciones por auditores externos a la entidad. Lo cual permitirá tener plena certeza del funcionamiento de los procesos que se ejecutan en la entidad. Posteriormente las personas implicadas en las decisiones correctivas tomaran las medidas adecuadas a los hallazgos encontrados por estos.			

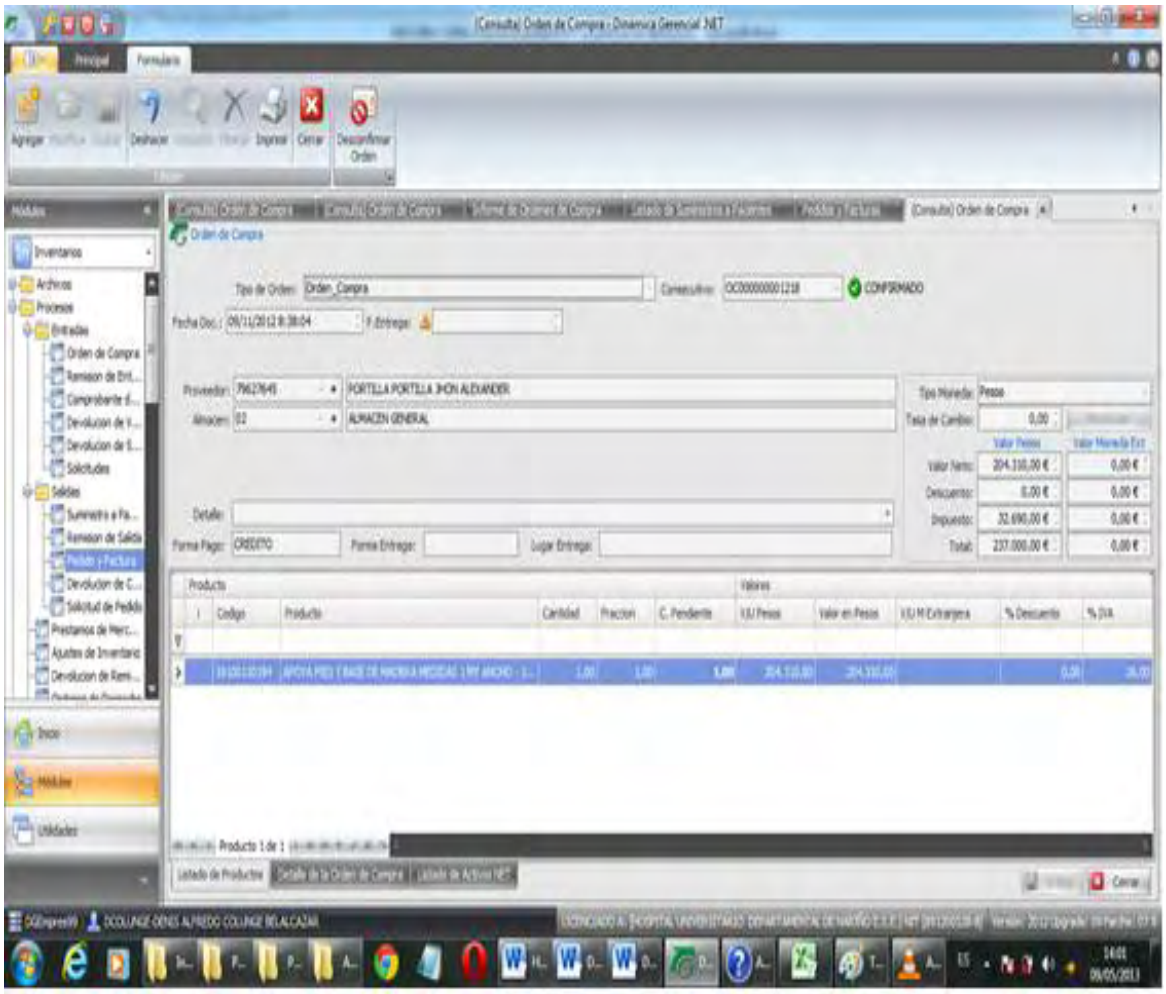
Fuente: Este proyecto

4.2.6 Pruebas al módulo de inventario

4.2.6.1 Entradas al módulo de inventarios. Las entradas al módulo de inventario están compuestas por directas e indirectas, lo cual convierte a este módulo en una columna vertebral del DGH.

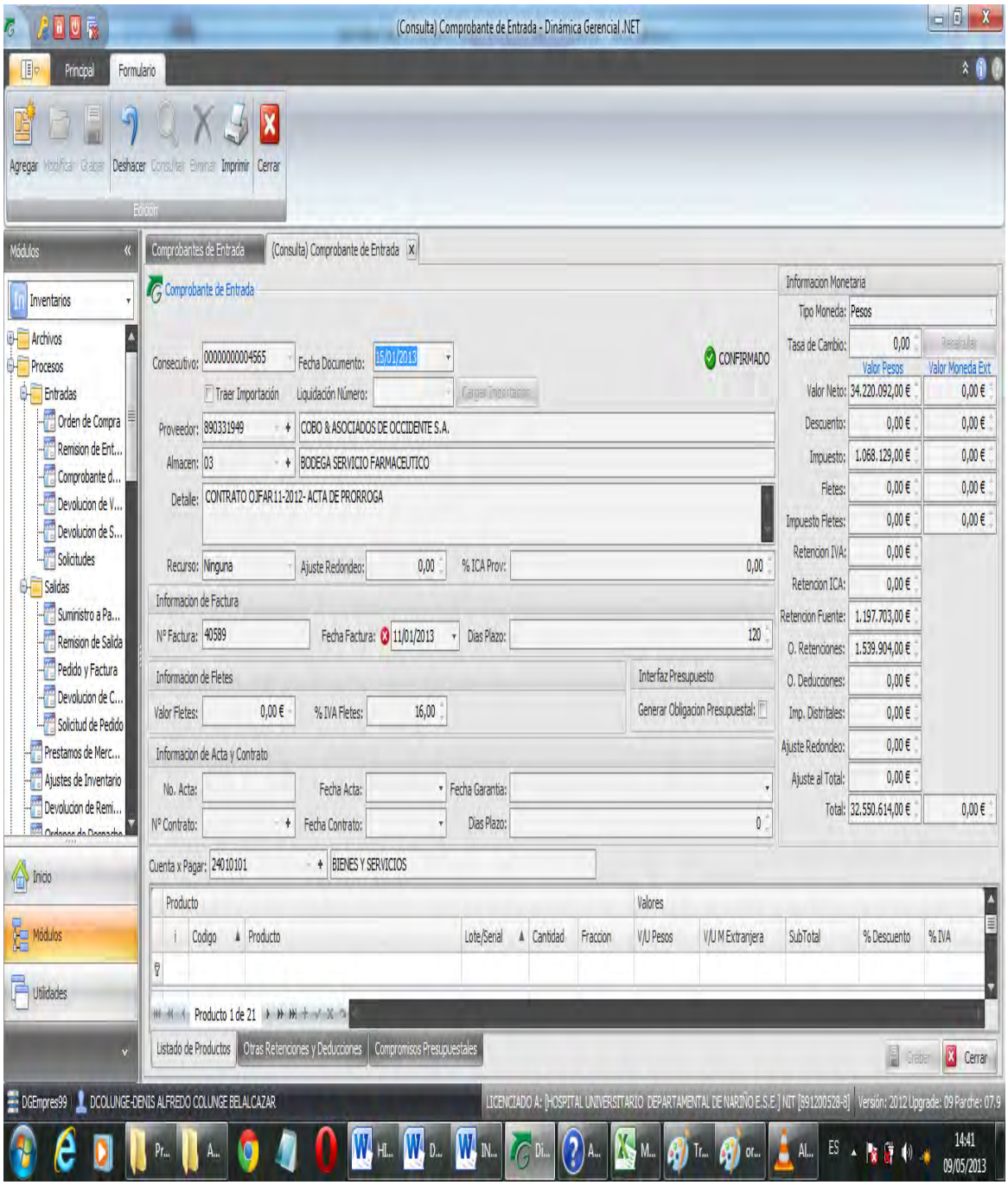
Entradas directas: son las que se realizan en este módulo. Tales como ordenes de compras, comprobantes de entrada, remisión de entrada, devoluciones de ventas, devoluciones de suministros y solicitudes de entradas, siendo las dos primeras las más utilizadas en los almacenes. Las demás son utilizadas en recursos farmacéuticos.

Figura 20. Orden de compra



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Figura 21. Comprobante de entrada

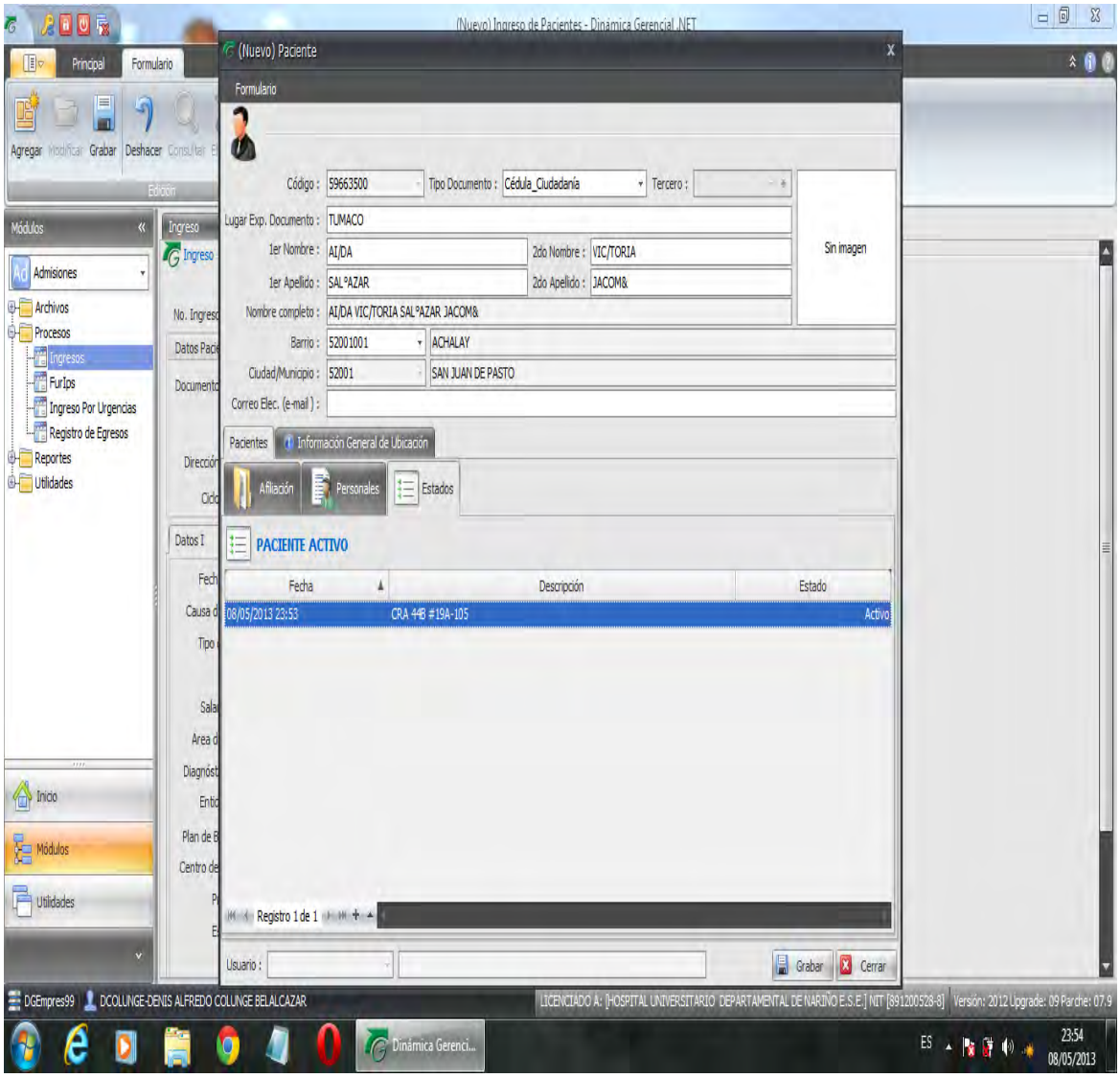


Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Entradas indirectas: son las que se realizan desde otros modulo por lo general de historias clínicas y admisiones, tales como ingreso a un paciente. Lo cual afecta a inventario y a gran parte del DGH motivo por el cual fueron estas las indicadas para probar la trazabilidad de la información.

En la figura ingreso a paciente el área encargada diligencia el formato de ingreso, con información personal y primordial del paciente en el módulo de admisiones.

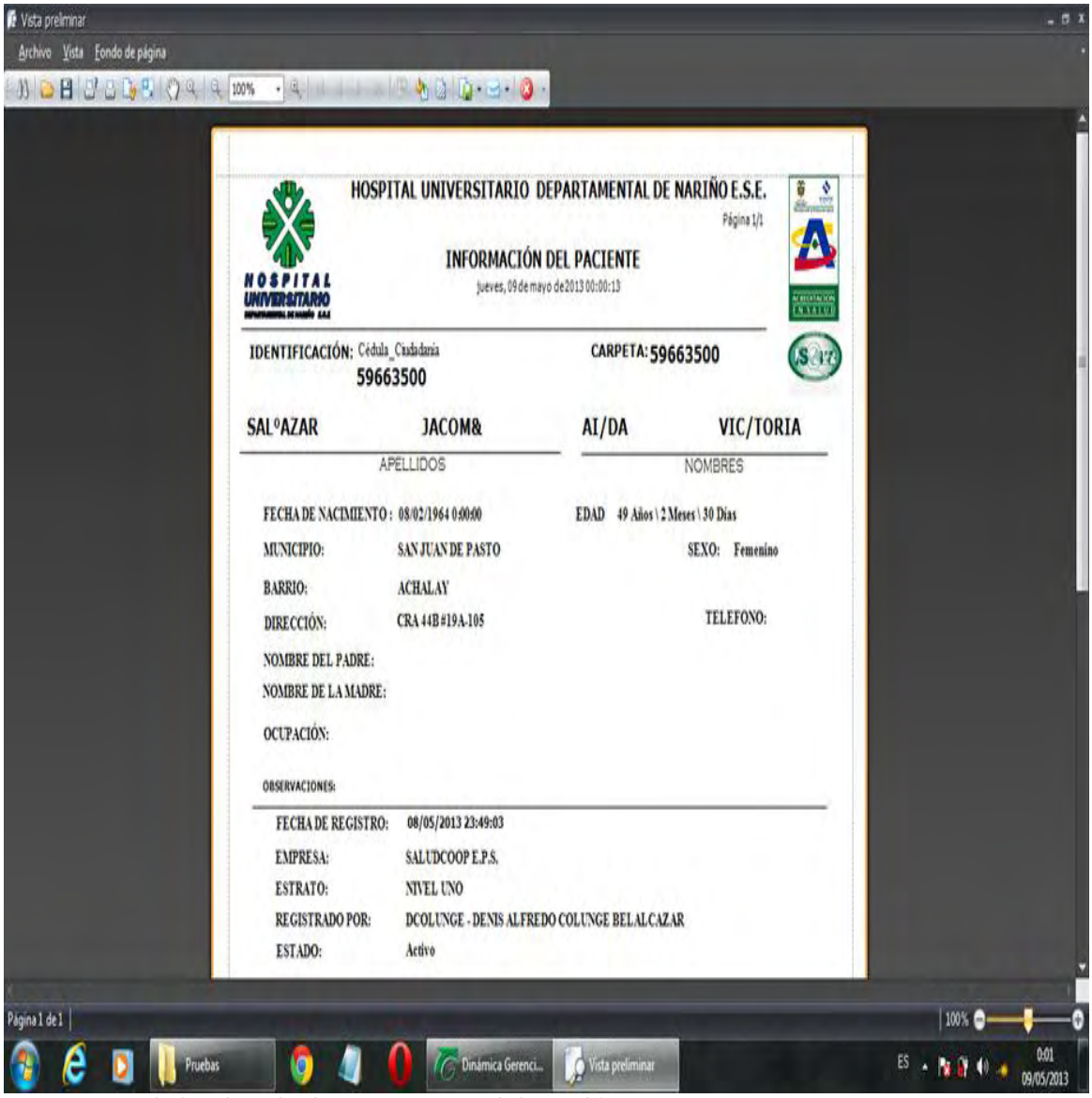
Figura 22. Ingreso a paciente



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.2.6.2 Salidas del módulo de inventarios. Las salidas en el módulo de inventario son coherentes con las entradas del mismo. Salvo algunos errores de validaciones en las cajas de texto en los campos de nombres y apellidos los cuales permiten (/°& etc.). Observar figura 22.

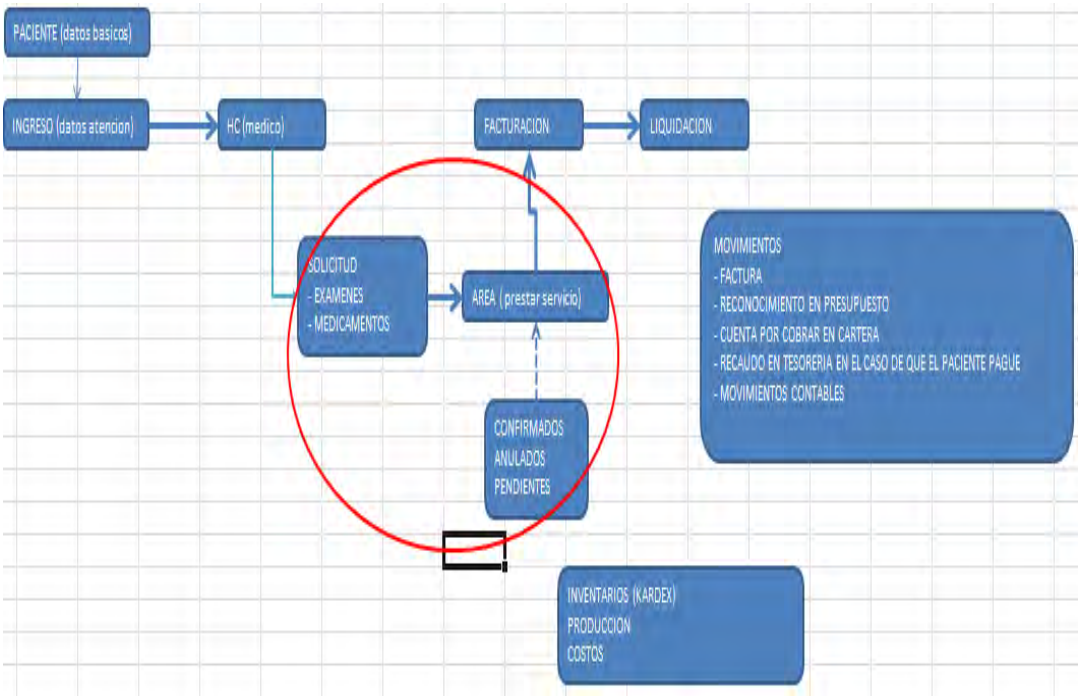
Figura 23. Informe de paciente



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.2.6.3 Trazabilidad de información en el módulo de inventarios del DGH

Figura 24. Trazabilidad

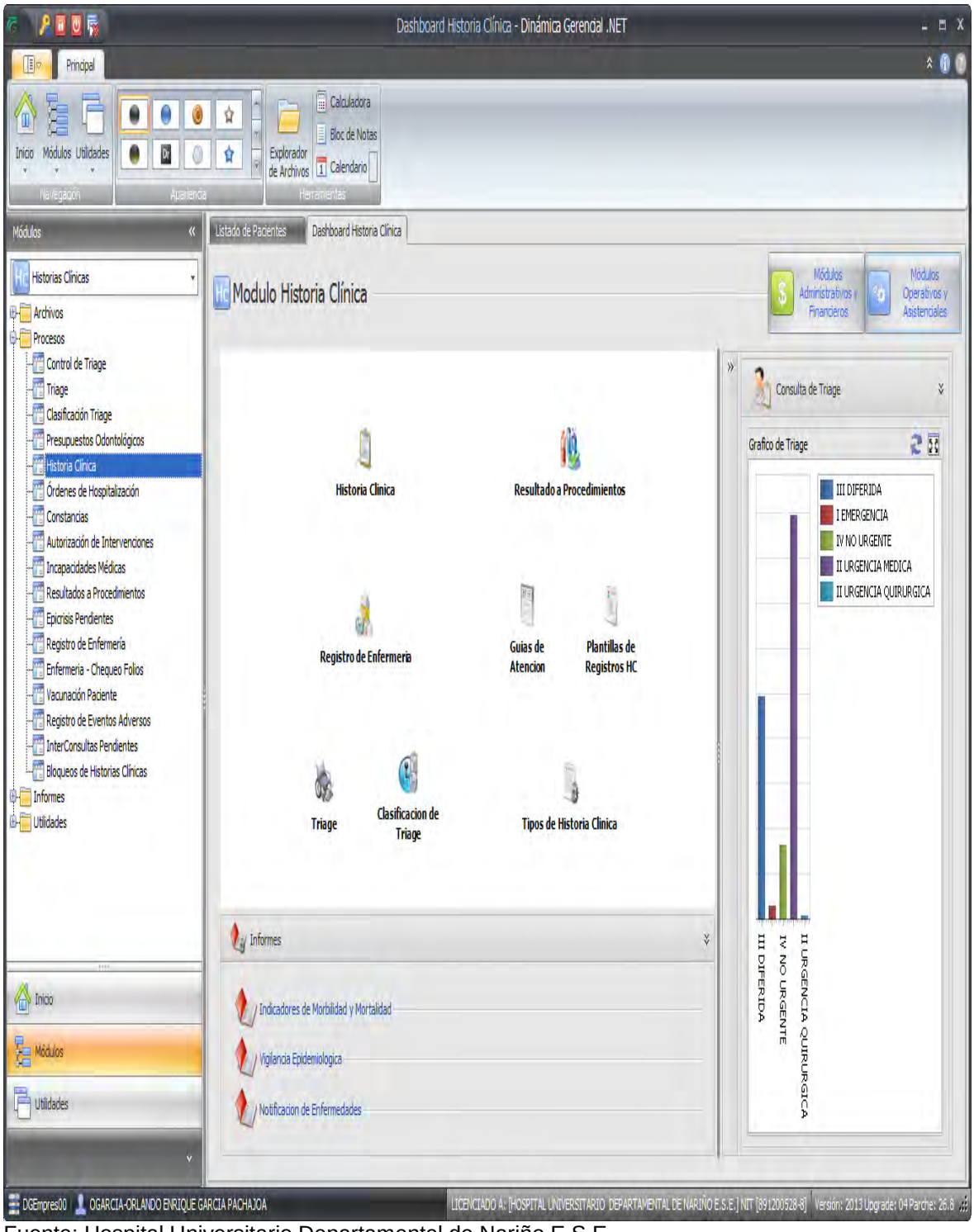


Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Para realizar la trazabilidad de la información en el módulo de inventario se tomó un ingreso de un paciente tanto de datos personales como datos primordiales de atención al paciente. Posteriormente el médico utiliza el módulo de Historias Clínicas para otorgarle ya sean medicamentos o exámenes según lo determine este. Una vez realizado el ingreso de información del paciente se actualiza el módulo de inventarios permitiéndole a recursos farmacéuticos confirmar, anular o dejar pendientes dichos medicamentos. Estos procesos en inventario actualizan facturación, lo cual genera movimientos en contabilidad, reconocimiento en presupuesto y cuentas por cobrar en cartera.

A continuación, observar las siguientes figuras: El médico ejecuta el módulo de Historias Clínicas, tal como se observa en la figura 25, solo si ya se le ha hecho el previo ingreso al paciente en el módulo de Admisiones; caso contrario el medico no podrá solicitar la droga del paciente.

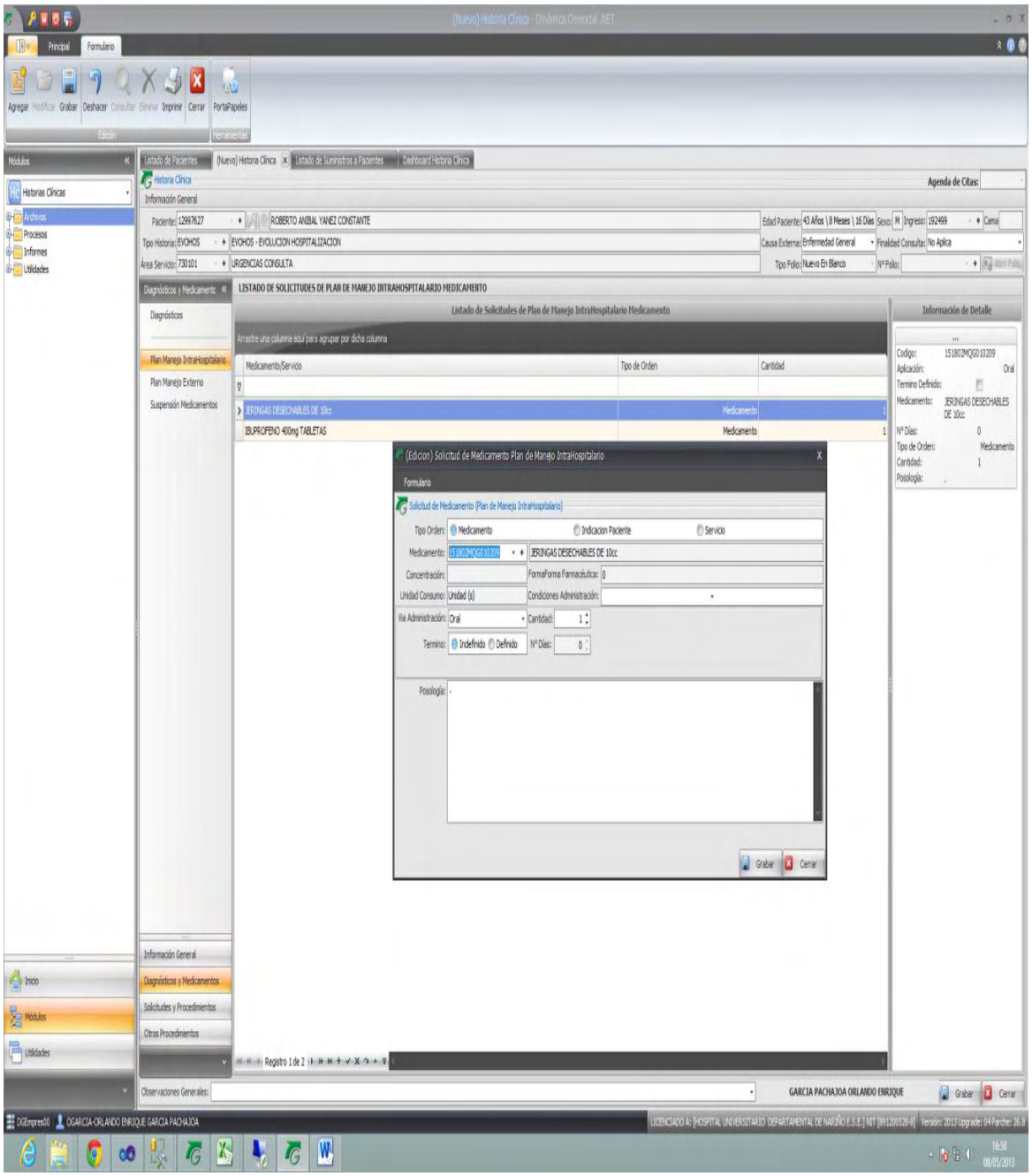
Figura 25. Diligenciamiento y solicitud de servicios



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Posteriormente, el médico después de haber ejecutado el módulo de Historias clínicas debe seleccionar el Plan Manejo IntraHospilario, el cual le permite solicitar los medicamentos para el paciente.

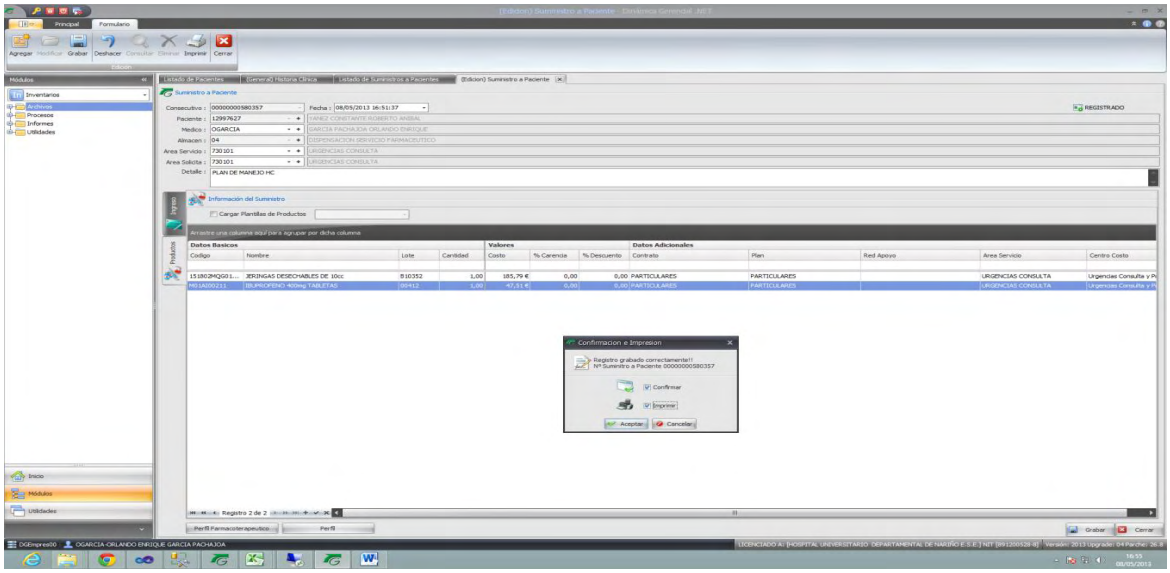
Figura 26. Plan de manejo intrahospitalario



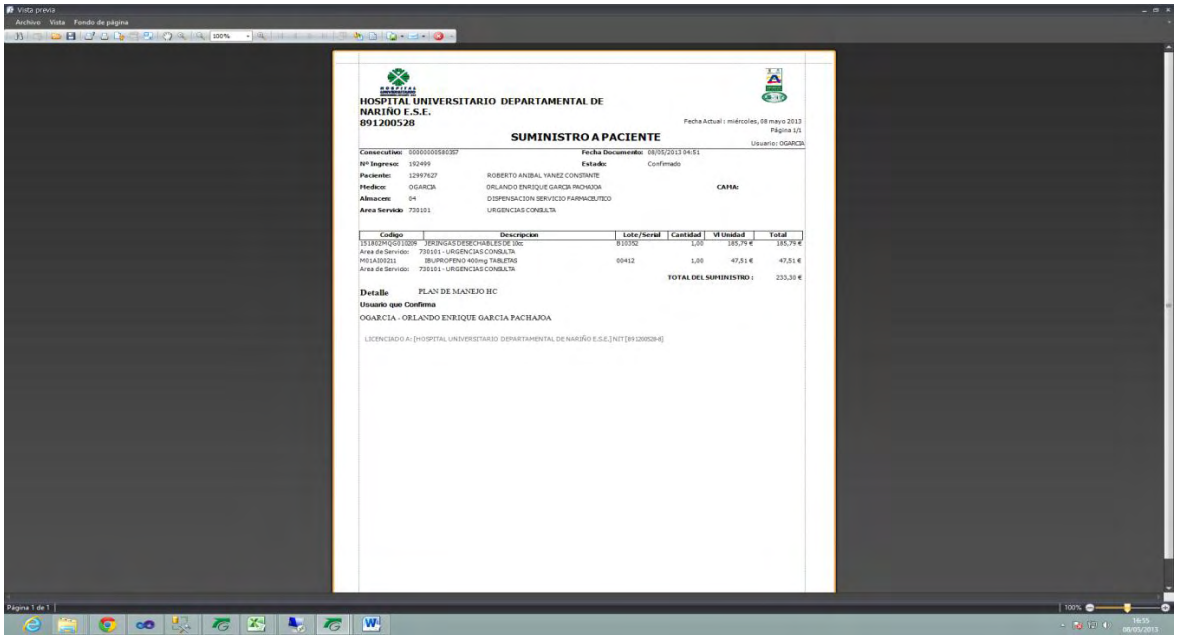
Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Luego la información suministrada por el médico en Historias Clínicas se actualiza en Recursos Farmacéuticos, donde solo bastara con ingresar en la tabla Listado de Suministros a Pacientes, lo cual permite observar los pedidos realizados por los diferentes médicos del HUDN.

Figura 27. Suministro a Paciente



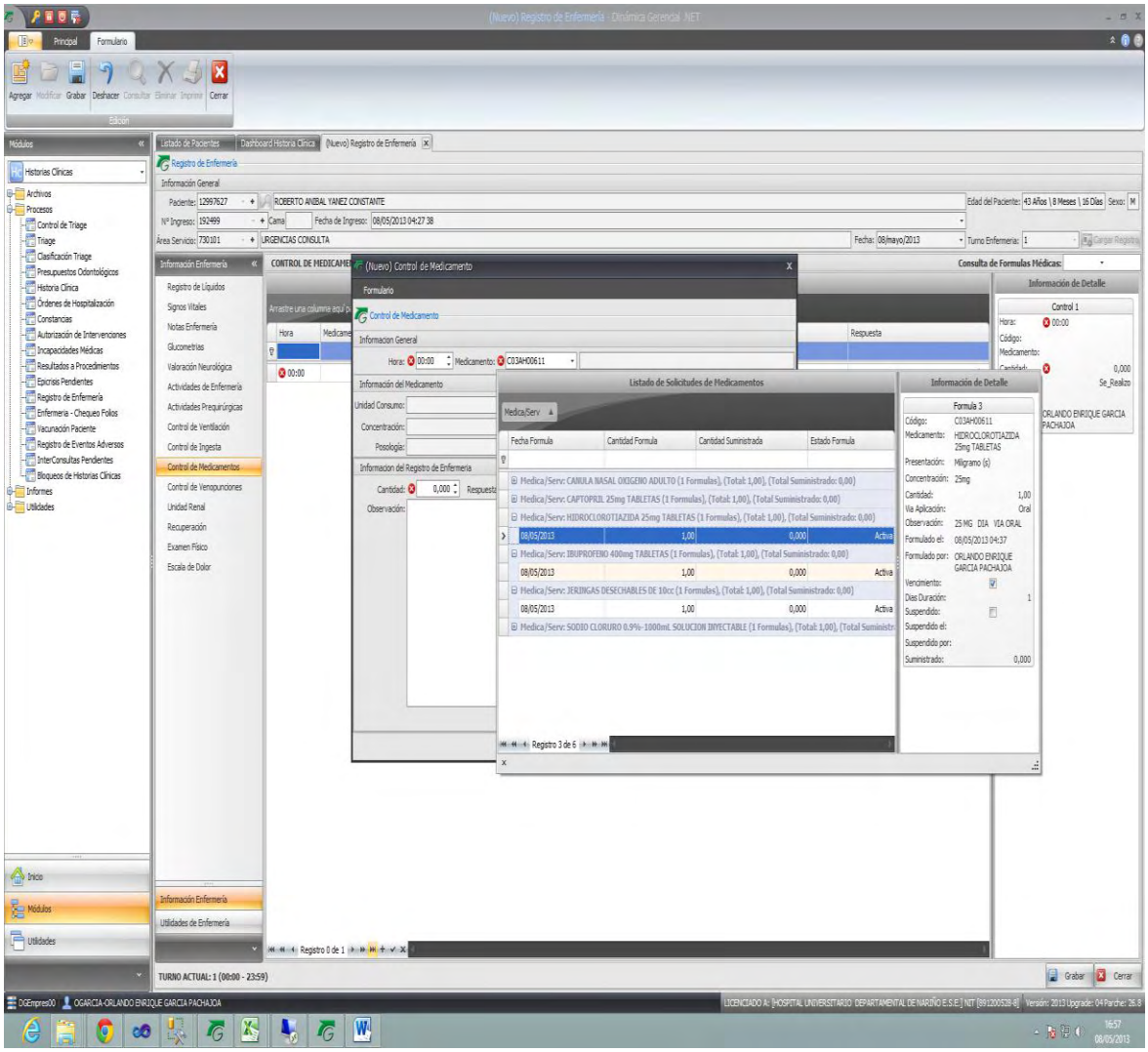
Continuación de Suministro a Paciente



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Los médicos pueden adquirir los diferentes medicamentos por medio de plantillas si lo desea o búsqueda general, además pueden editarlos o anularlos. El DGH no posee control con la cantidad de medicamentos solicitados ya que el medico puede pedir cantidades no normales lo cual afecta la eficiencia del proceso.Por otro lado al anular medicamentos el DGH no permite justificar la anulación de los medicamentos. Además cuando un suministro a paciente se anula este aparece en Farmacia y registro de enfermería para aplicarlo al paciente, algo que no debe suceder.

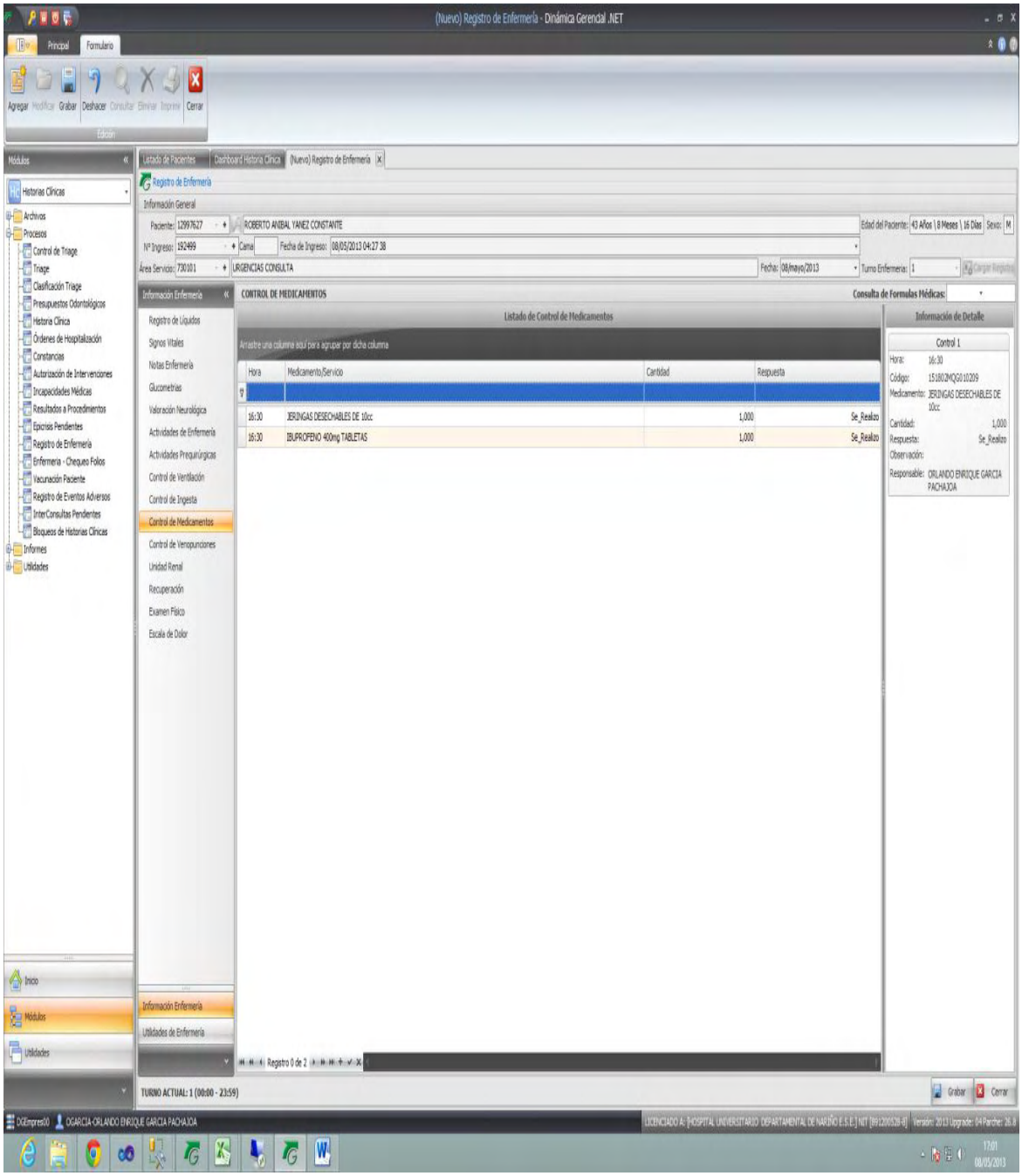
Figura 28. Control de medicamentos



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

En la opción registro de enfermería del módulo de Historias Clínicas se puede editar la cantidad de medicamentos.

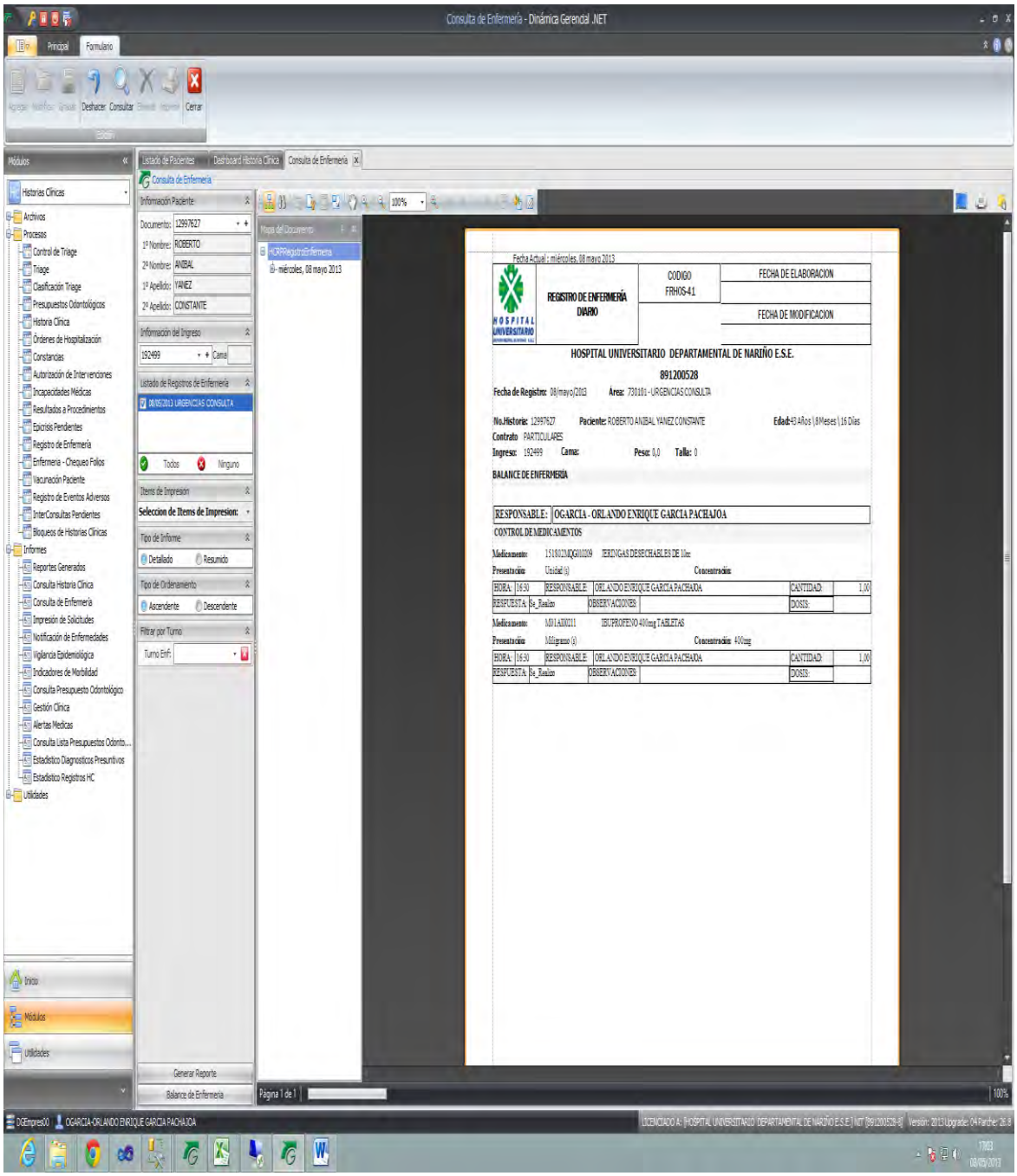
Figura 29. Cantidad de medicamentos



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

En este formulario el médico podrá imprimir la droga suministrada al paciente

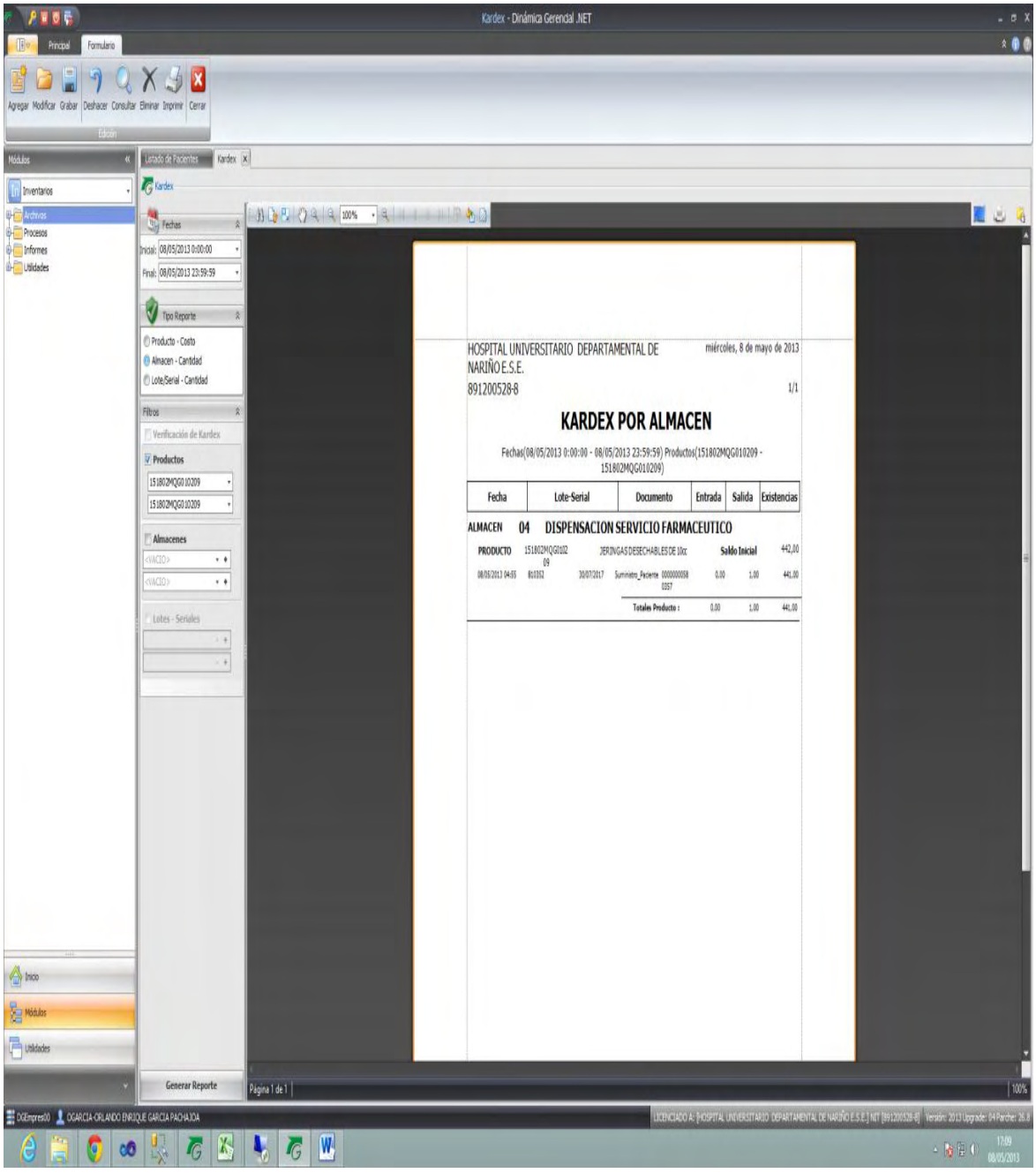
Figura 30. Registro de enfermería



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Una vez se actualiza el módulo de inventario se puede verificar en el KARDEX los movimientos realizados por las áreas prestadoras de servicios.

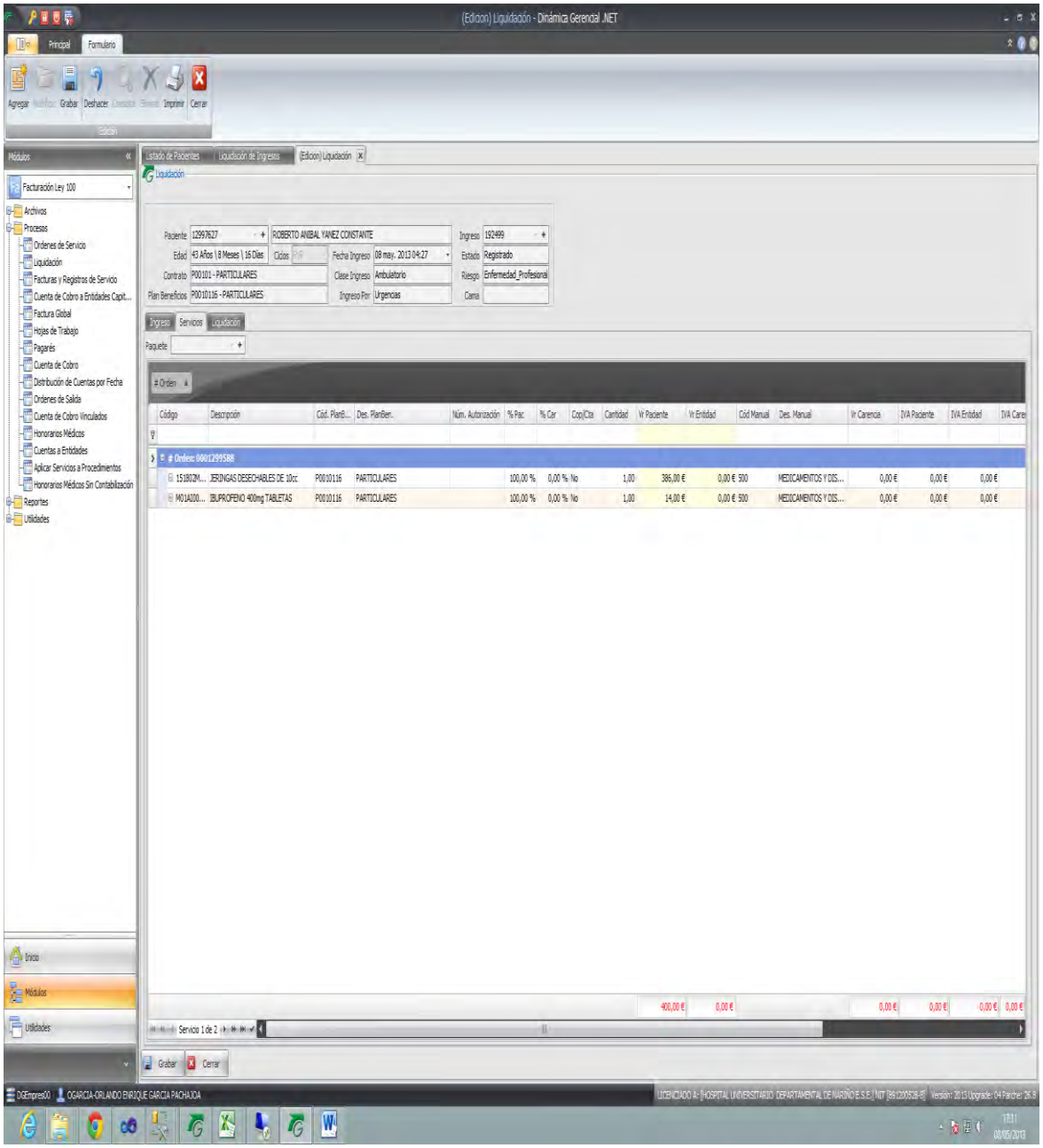
Figura 31. Registro en KARDEX



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

En la Figura 32. Se observa la actualización del módulo de Facturación Ley 100 con las drogas solicitadas por el médico, con su respectivo valor unitario. Cabe aclarar que el valor no está en pesos colombianos esta en euros, cosa que debe solucionar SYAC.

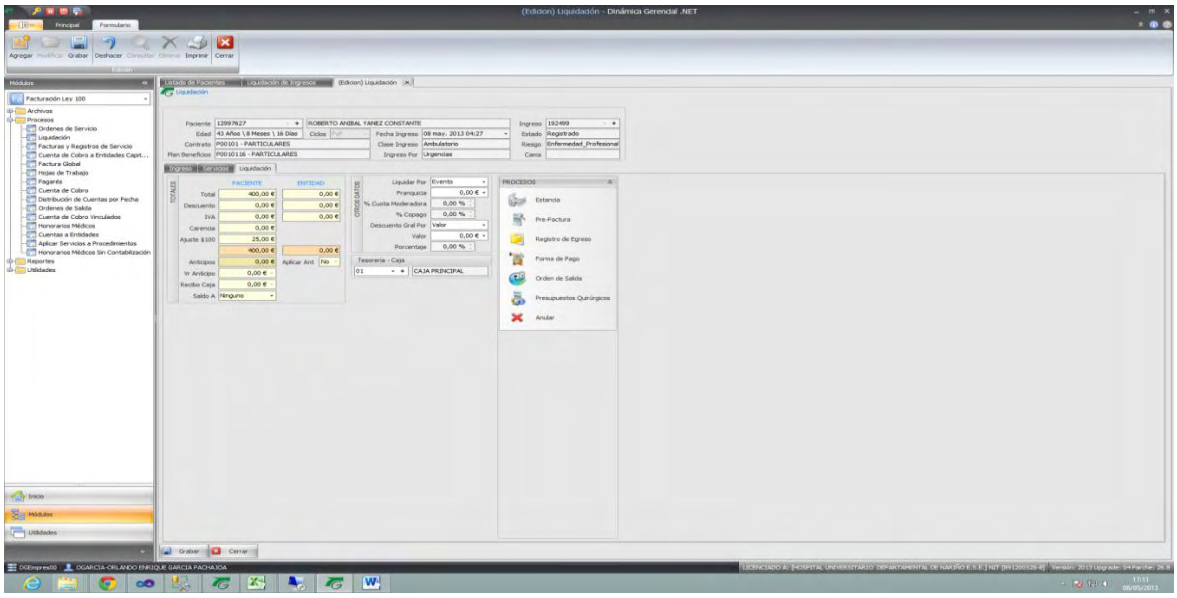
Figura 32. Facturación



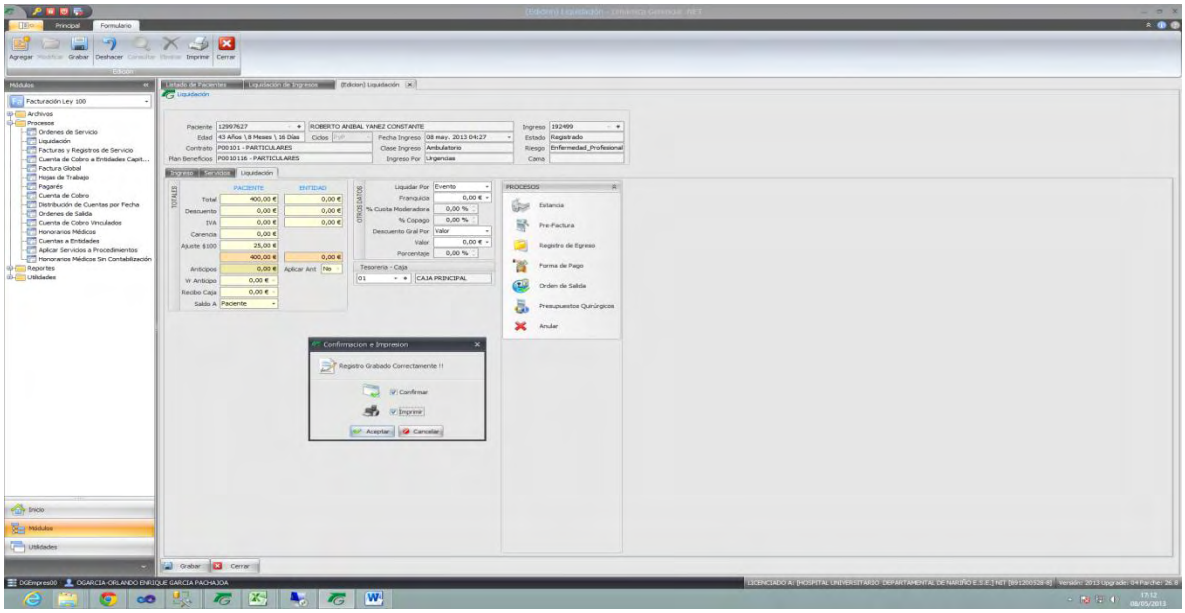
Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Una vez actualizado el módulo de facturación y mediante la opción liquidación, se procede a imprimir la factura de venta de los medicamentos, los cuales han sido registrados exitosamente por el médico. Luego se genera una cuenta por cobrar en cartera, un recaudo en tesorería en caso de que el paciente pague y por último se realizan movimientos contables.

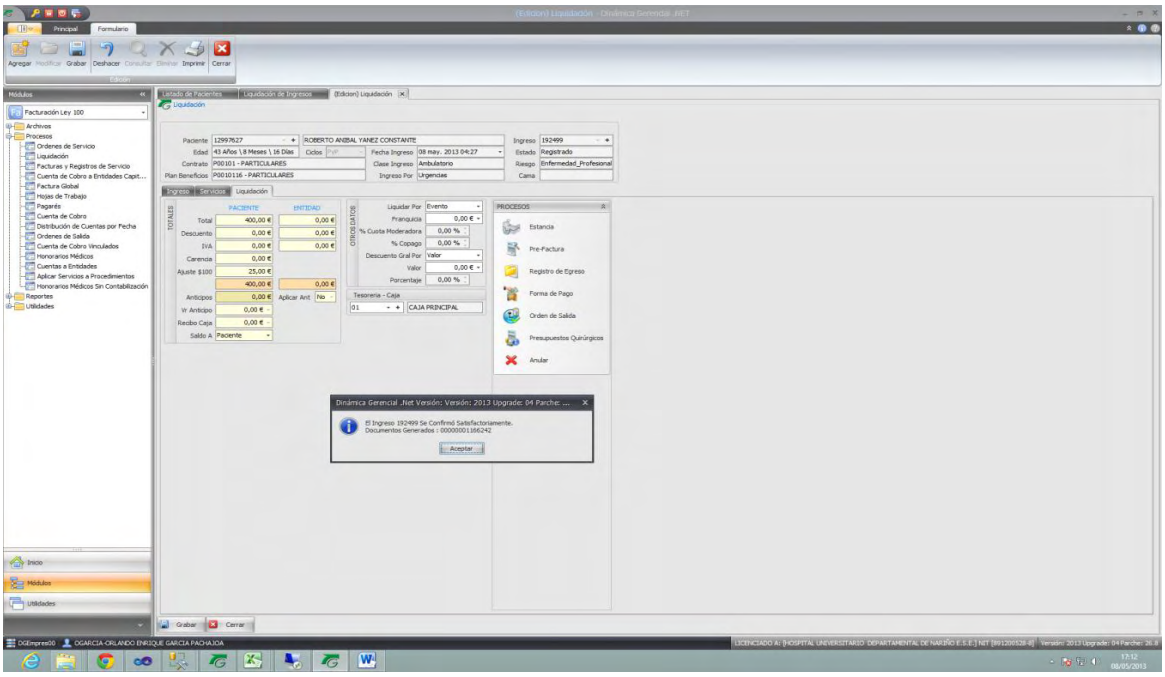
Figura 33. Liquidación



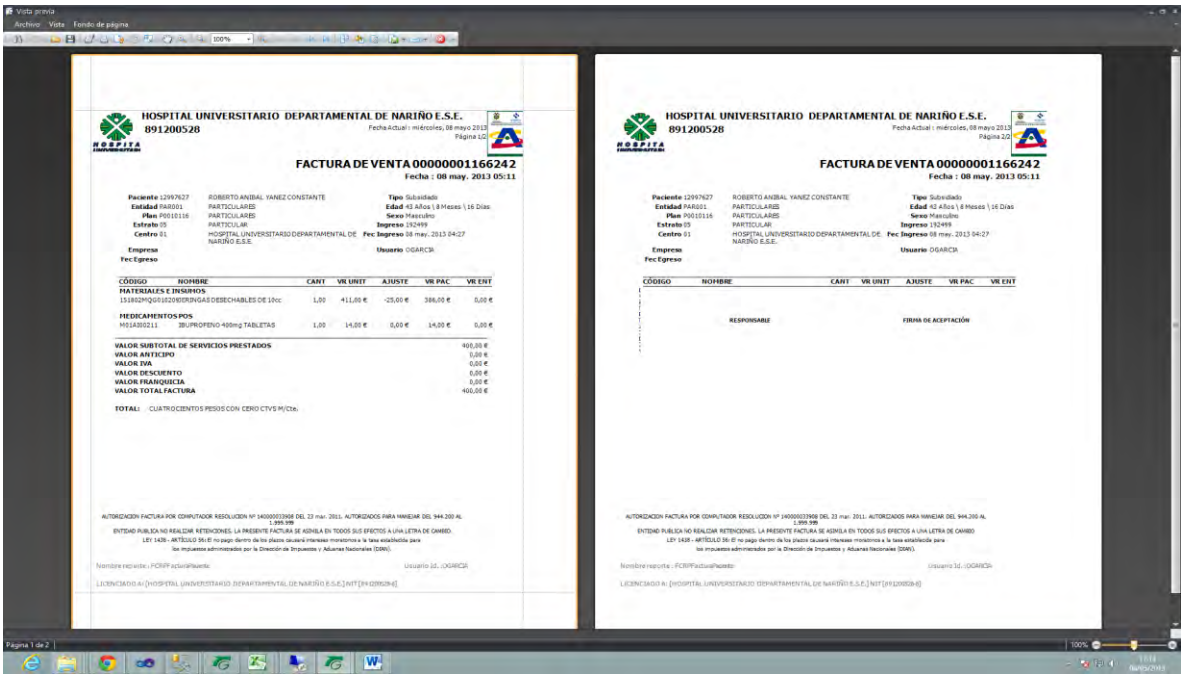
Continuación de Liquidación



Continuación de Liquidación



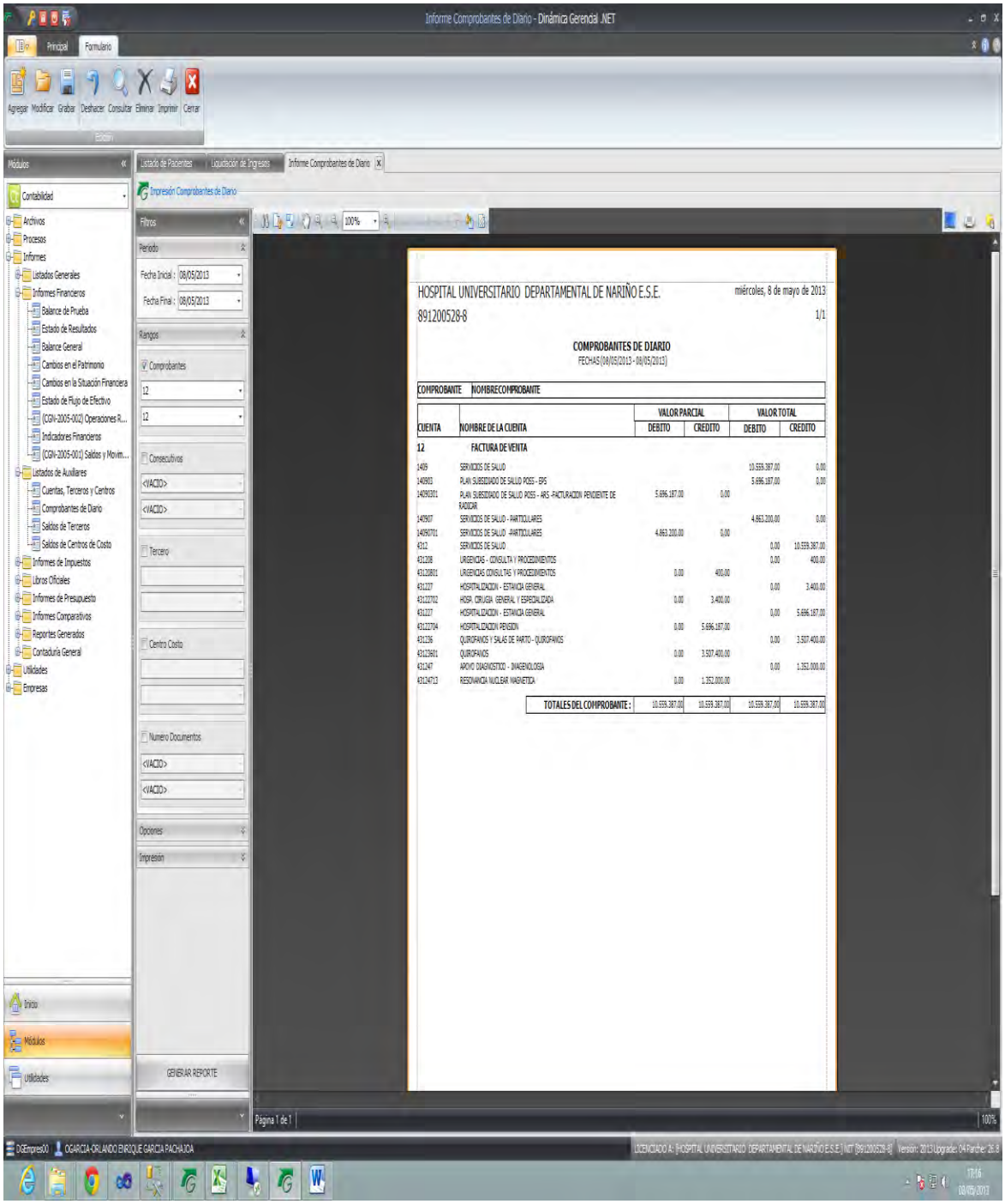
Continuación de Liquidación



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

Por último, se realizan los movimientos contables realizados en la trazabilidad de la información.

Figura 34. Contabilidad



Fuente: Hospital Universitario Departamental de Nariño E.S.E.

4.2.7 Informe Final del Proyecto de auditoría

Objetivo General

Evaluar la eficiencia y eficacia del módulo de inventario del Sistema de Información del Hospital Universitario Departamental de Nariño para coadyuvar en su buen funcionamiento.

Objetivos Específicos

- Identificar el funcionamiento de las entradas al módulo de inventario.
- Analizar las salidas de informes generados por el módulo de inventario.
- Efectuar un seguimiento riguroso a toda la trazabilidad de la información del módulo de inventario.
- Establecer estrategias de mejoramiento al módulo de inventario del Hospital Universitario Departamental de Nariño.

Limitaciones Durante la Ejecución del Proyecto

La auditoría se realizó de manera normal y adecuada, se contó con la colaboración de los funcionarios del Hospital Universitario Departamental de Nariño para la realización de entrevistas y cuestionarios.

4.2.7.1 Visión General de la metodología empleada en la auditoría. En primer lugar se realizado visitas al Hospital Universitario Departamental de Nariño, con el objeto de hacer un estudio preliminar tanto de los aspectos de infraestructura física (áreas, equipos, red, cámaras, servidores) como del Sistema de Información Dinámica Gerencial Hospitalaria el cual es el contexto para el desarrollo de la auditoria.

4.2.7.2 Enfoque general de las herramientas utilizadas. Para la realización de este proyecto se utilizó el COBIT (*Control objectives for information and related technology*), el COBIT es una herramienta práctica para evaluar los sistemas de información dentro de una empresa ya sea pública o privada. Está soportado bajo la filosofía de que los recursos de TI de una organización deben ser evaluados por un conjunto de procesos agrupados para hallar la información actual de la institución y coadyuvar en sus metas. En cuantos a su estructura, el Cobit es como un árbol. Es decir posee unos niveles, los cuales permiten al auditor decidir cuales dominios y procesos tomar de acuerdo a las necesidades que tenga o quieran que se evalúen en la entidad.

❖ Dominios: conjuntos de procesos.
❖ Procesos: conjunto de objetivos de control.
❖ Objetivos de control: conjunto de actividades las cuales le permiten al auditor elaborar los cuestionarios cuantitativos y entrevistas entre otros.

4.2.7.3 Resultados obtenidos durante el proceso de la auditoría

Hospital Universitario Departamental de Nariño

Posteriormente se puntualizan hallazgos y recomendaciones para cada uno de los procesos evaluados del COBIT durante este proceso en el Hospital.

Dominio 1. (PO) Planear y organizar

Proceso (PO2) Definir la Arquitectura de la Información

Hallazgos

➢ No existe un manual de sistema técnico.
➢ No existen procedimientos para dar soporte efectivo a la administración de la información.
➢ No existe una sistematización total de los procesos en el hospital.
➢ La calidad de TI en su totalidad no es apropiada para la entidad.

Recomendaciones

✓ En las próximas adquisiciones tecnológicas del HUDN se recomienda que en el contrato con SYAC se establezca la entrega del manual de sistema técnico, donde se especifiquen con lujos y detalles todas las características técnicas del software.
✓ Documentar todos y cada uno de los procesos que se lleven a cabo en la administración de la información.
✓ Realizar una sistematización de casi todos los procesos, salvo aquellos que realmente no se puedan sistematizar.
✓ Utilizar un solo tipo de tecnología, con el objeto de evitar incompatibilidades que disminuyan el rendimiento de estas.

Proceso (PO3) Determinar la Dirección Tecnológica

Hallazgos

- No existen técnicas de migración de datos.
- No existe un área de sistemas segura.
- No existe un comité técnico de sistemas.

Recomendaciones

✓ Documentar todo el proceso de migración de datos, para que con facilidad otros peritos no tengan ningún inconveniente al momento de realizar este proceso.
✓ Implementar un proyecto de construcción de un área de sistemas segura, en la cual solo el personal autorizado tenga acceso a la información. No como la actual que cualquiera puede tener acceso si así lo decide.
✓ Crear un comité técnico de sistemas que en el recaiga toda la responsabilidad de asesoría y documentación de los procesos del área de sistemas.

Proceso (PO7) Administrar Recursos Humanos de TI

Hallazgos

- No existe una verificación periódica del personal en sus funciones.
- No existen programas de calificación y certificación de los usuarios de DGH.
- No existe una asignación de roles rigurosa.
- No existe un documento de garantía, que exprese que el personal del Hospital y específicamente los que trabajan en el DGH coadyuven a mitigar riesgos de este.

Recomendaciones

✓ Realizar verificaciones periódicas al personal, respecto a su desempeño en las funciones y como está elaborando los procesos.
✓ Implementar programas de calificación y certificación de los usuarios del DGH, y un entrenamiento periódico del personal.
✓ Otorgar roles serios a los usuarios del DGH en el módulo de inventario, es decir que solo se les debe habilitar del sistema lo que necesite el usuario para el desarrollo de sus actividades propuestas por el jefe. No como en la actualidad, algunos usuarios no hacen uso de otro segmento del sistema por solo respeto e

intuición de que puede estar mal el uso no autorizado de un rol que no les compete.

✓ Hacer la transferencia del conocimiento, reasignar responsabilidades y eliminar los privilegios de accesos a la información, de esta manera se elimina la dependencia y riesgos actuales, presentes y futuros.

Proceso (PO9) Evaluar y Administrar los Riesgos de TI

Hallazgos

➢ No existe un plan de recuperación y minimización del impacto en los procesos del Hospital que garanticen la continuidad del funcionamiento del Módulo de Inventario del DGH.
➢ El Hospital no cuenta un plan de mitigación de riesgos del Sistema de Información DGH.
➢ No existe un procedimiento que en el cual se verifique que la construcción, prueba e implantación de los controles y procedimientos de seguridad sean formalmente aprobados antes de que se utilice el sistema información **DGH.**

Recomendaciones

✓ Implementar un repositorio digital donde se almacenen todos los documentos pertinentes de los procesos manejados en el área de sistemas.
✓ Realizar un plan de mitigación de riesgos donde se especifique todos y cada uno de los sectores del HUDN que están propensos a un eventual siniestro, y evaluar el impacto que causaría en caso de ocurrir.
✓ Se recomienda que al momento de establecer el contrato con SYAC que les faciliten todas las pruebas realizadas a este software.

Dominio 2. (AI) Adquirir e Implementar

Proceso (AI3) Adquirir y Mantener Infraestructura Tecnológica

Hallazgos

➢ El hospital no cuenta con un plan de mantenimiento de la infraestructura tecnológica que garantice que se están controlando los cambios tecnológicos.
➢ El área de sistemas del Hospital no se encuentra en la capacidad, de estar a la vanguardia de optimizar el sistema, de manera productiva y segura.
➢ No existe una adecuada seguridad, integridad, y disponibilidad, de la infraestructura TI en el Hospital

Recomendaciones

✓ Crear un plan de mantenimiento que permita tener la certeza y rigor de las actividades de mantenimiento. Además que se estén efectuando en el tiempo oportuno e indicado, y a su vez una correcta documentación de todas las incompatibilidades encontradas y las correcciones de las mismas.
✓ Empezar por documentar todos los procesos que se hagan respecto a infraestructura tecnológica, los parches que se le hagan al sistema, las auditorías internas con claridad y autonomía en sus reportes, administrar de manera rigurosa los roles del sistema, entre otros.
✓ Empezar por conseguir seguridad, integridad, y disponibilidad adecuada, corrigiendo todas y cada una de las faltas que posee la infraestructura de la entidad teles como:

- La red de la entidad cuenta con distintos tipos de tecnología como: cableado, switches, etc. lo cual es un factor de disminución de rendimiento en la tecnología utilizada.
- El riesgo que se corre si algún usuario del sistema le da por hacer pruebas e ingresar valores en las opciones que tiene habilitadas.
- Establecer cámaras en lugares estratégicos. Es decir en la parte donde está el servidor principal, además de estar al lado de la central eléctrica.

Proceso (AI7) Instalar y Acreditar Soluciones y Cambios

Hallazgos

➢ Cuándo se está implantando un nuevo sistema en el Hospital, o se está modificando un sistema ya existente, no se cuenta con un plan para la implantación de este, y un plan de respaldo vuelta atrás.
➢ No existe una evaluación de las pruebas practicadas a los sistemas por parte de la gerencia del Hospital.
➢ No se realizan revisiones al sistema de información luego de la implantación o modificación del sistema actual.

Recomendaciones

✓ Crear un plan documentado para la implantación y plan de respaldo vuelta atrás de los sistemas de la entidad. El plan debe definir claramente el diseño de versiones, construcción de paquetes de versiones, procedimientos de implantación e instalación, manejo de incidentes, controles de distribución, almacenamiento de software, revisión de la versión y documentación de cambios.
✓ La gerencia debe solicitar que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año. La gerencia debe estar involucrada en el proceso de adquisición de los sistemas, no solo gerencia de información. Esto le permitirá a gerencia garantizar que los procesos con los cuales está funcionando la empresa están a acorde con los estándares de calidad perseguidos por el hospital.
✓ Realizar revisiones periódicas al sistema, lo cual permitirá hallar los errores que se puedan presentar en la ejecución del sistema montado.

Dominio 3. (DS) Entregar y Dar Soporte

Proceso (DS5) Garantizar la Seguridad de los Sistemas

Hallazgos

➢ Los servidores no están asegurados físicamente
➢ Las contraseñas no se cambian periódicamente de acuerdo al programa establecido.
➢ No es observada a plenitud la seguridad de archivos y de la base de datos.
➢ No se garantiza que se utilicen técnicas de seguridad y procedimientos de seguridad asociados para autorizar accesos y controlar los flujos de información desde y hacia la red.

Recomendaciones

✓ Crear lo antes posibles un área segura para posesionar los servidores de la entidad.
✓ Realizar un cambio periódico de las contraseñas en la entidad, para evitar sabotajes cibernéticos, y concientizar a los usuarios de que la clave de acceso no prestar. Respecto al acceso al servidor principal de la entidad encriptar la clave y serrar puertos en lo más que se pueda.
✓ Crear controles de seguridad de manera inmediata en los servidores, y especialmente en el servidor principal donde se encuentra la base de datos de la organización, la cual contiene toda la información de la entidad. Deben tener en cuenta el almacenamiento en la nube.
✓ No deben tener acceso a la DB tantos peritos; documentar los proceso que lleve la persona que esté a cargo para no crear dependencias de este.
✓ Implementar técnicas y metodologías de seguridad en la red para proteger la información de manera adecuada y segura tales como: pasar todos los servidores a ambiente Linux, al menos el principal. Por otro lado contar con software de detección de instrucciones, firewalls y segmentación de la red.

Proceso (DS12) Administración del Ambiente Físico

Hallazgos

➢ No se definieron ni diseñaron centros de datos para el equipo de TI ni se tuvieron en cuenta las normas de seguridad física y las leyes de seguridad física en el trabajo.

Recomendaciones

✓ Rediseñar un centro de datos y tener en cuenta todos los factores de riesgos que incurriría la organización. Se recomienda que exista un complemento paciente -información. Que no solo la prioridad sea el paciente sino también la información.

Dominio 4. (ME) Monitorear y Evaluar

Proceso (ME2) Monitorear y Evaluar el Control Interno

Hallazgos

- No se monitorea la eficiencia y eficacia de la auditoría interna.
- No existe una identificación de las excepciones de control, ni se identifican sus causantes, ni se reportan a los interesados.
- No existe la evaluación de control interno por parte de terceros.

Recomendaciones

✓ Monitorear la eficiencia de estas auditorías y permitir mostrar y documentar todas las anomalías encontradas en estas.
✓ Reportar tanto al jefe de área como a gerencia de todas las anomalías encontradas en la auditoría interna, para que se tomen todas las correcciones del caso y así cumplir con la misión y visión de la entidad.
✓ Realizar evaluaciones por auditores externos a la entidad. Lo cual permitirá tener plena certeza del funcionamiento de los procesos que se ejecutan en la entidad. Posteriormente las personas implicadas en las decisiones correctivas tomaran las medidas adecuadas a los hallazgos encontrados por estos.

CONCLUSIONES

Durante el proceso de auditoría al módulo de inventario del sistema de información del Hospital Universitario Departamental de Nariño, se pudo concretar diferentes criterios y pruebas con respecto a aspectos como entradas, salidas, trazabilidad, seguridad física y lógica de la información de la entidad. Lo cual permitió realizar recomendaciones adecuadas para cada uno de estos elementos evaluados.

Se puede concluir que las auditorías a sistemas de información son el único proceso que a través de una serie de procedimientos metódicos de análisis, observación y ejecución permiten establecer hallazgos, secuelas, riesgos, falencias y sus posibles recomendaciones a estos factores revelados por la institución auditada; permitiéndoles a los dirigentes encargados de tomar las decisiones, proponer un plan de mejoramiento detallado de todas y cada una de las anomalías encontradas en el proceso de evaluación a la entidad, y posteriormente ejecutar este plan para obtener excelentes resultados.

Las entradas de datos al módulo de inventario del Sistema de Información son inadecuadas en el almacén debido a que no se utiliza el DGH para recibir las diferentes solicitudes expedidas por las áreas del Hospital Universitario Departamental de Nariño, sino que se realizan por medio de papel. Lo cual provoca errores humanos al momento de ingresar los pedidos al sistema, y a su vez incoherencias en los cálculos de los productos.

El proceso de entrada, salida y trazabilidad de la información en la entidad es eficaz, ya que permite hacer las actividades diarias de la organización, pero no se realizan con la mayor seguridad del caso, debido a que los roles en el DGH no están siendo administrados de la mejor manera, lo cual puede ocasionar serios problemas tanto actuales como futuros. Por otro lado las excepciones del DGH no están bien manejadas.

Se puede concluir que en la organización no existe una política en la cual se especifiquen los procesos realizados en el área de sistemas, los cuales deben ser claramente documentados, con el objeto de generar independencias de peritos y tener acceso a los procesos en cualquier momento o situación; obteniendo como resultado agilidad y disminución de tiempo al realizar otro profesional este proceso.

RECOMENDACIONES

Establecer controles de seguridad rigurosos tanto en la base de datos de la entidad como en el DGH, los cuales le brinden a la institución una convicción en la administración de la información y posteriormente le coadyuven a mitigar unos de los riesgos más importantes para la empresa.

Realizar una reestructuración de la infraestructura tecnológica del HUDN. La red de la entidad está constituida por diferentes tecnologías, el cableado en algunos pisos es antiguo. Hay que realizar una migración a categoría 6 a toda la organización, y con una sola tecnología para que no haya problemas de incompatibilidades. Los servidores de la entidad deben estar en Linux al menos el principal y proponer un plan para la construcción de un centro de datos, con todos los requerimientos establecidos en las normas que integran esta parte, para así alcanzar niveles altos en calidad de administración de la información.

Hacer asignaciones de roles precisas, lo cual coadyuvará a disminuir riesgos en las entradas y salidas de los datos, con o sin intención de los usuarios del sistema. Además establecer políticas que garanticen la documentación de todos los procesos que se realicen en el área de sistemas, y a su vez un control adecuado a la seguridad de la red en la organización.

Realizar evaluaciones por auditores externos a la entidad. Lo cual permitirá tener plena certeza del funcionamiento de los procesos que se ejecutan en la entidad. De tal manera que permita a las personas implicadas en la toma de decisiones, diseñar un plan de mantenimiento ya sea preventivo o correctivo, el cual ayudara a alcanzar los objetivos propuestos por la organización con altos niveles de calidad y seguridad.

Crear un plan documentado para la implantación y plan de respaldo vuelta atrás de los sistemas de la entidad. El plan debe definir claramente el diseño de versiones, construcción de paquetes de versiones, procedimientos de implantación e instalación, manejo de incidentes, controles de distribución, almacenamiento de software, revisión de la versión y documentación de cambios.

BIBLIOGRAFÍAS

ARENS A, Alvín. Auditoria un enfoque integral. México: Prentice Hall, 1996.

MCLEOD, Raymond. Sistemas de información gerencial. México: Pearson Education, 2000.

MUÑOZ R, Carlós. Auditoría en sistemas computacionales. México: Pearson Education, 2002.

NETGRAFIA

ACOSTA, Mario. Norma Cobit. Disponible en Internet: http://nyxmario7.wordpress.com/2010/06/01/norma-cobit/ Consultado: Abril de 2013

Administración de la Calidad. Diseño de sistemas de calidad total. Disponible en Internet:http://www.itch.edu.mx/academic/industrial/admoncalidad/unidad05.html Consultado: Marzo de 2013

Archivos Auditoría en Sistemas. Estudio Inicial del Entorno Auditable. Disponible en Internet: http://archivosauditoria.blogspot.com/2009/11/estudio-inicial-del-entorno-auditable.html Consultado: Marzo de 2013

Archivo [pdf] COBIT 5, UN MARCO DE NEGOCIO PARA EL GOBIERNO Y GESTION DE LAS TI DE LA EMPRESA.-Adobe Reader.P.13.

Archivo [pdf] PLAN DE DESARROLLO, HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.-Adobe Reader.P.83.

Archivo [pdf] PORTAFOLIO DE SERVICIOS, HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.-Adobe Reader.P.11-27.

Asociación de Auditoría y control de Sistemas de Información. Normas Generales Para la Auditoria de sistemas de Información. Disponible en Internet: http://galeon.com/auditoriaycont/niads.pdf Consultado: Marzo de 2013

Auditores y asesores en contabilidad y sistemas. Alcance de la Auditoria Informática. Disponible en Internet: http://www.oocities.org/espanol/audiconsystem/auditori.htm Consultado: Marzo de 2013

BONILLA, Carmen. El Informe Coso. Disponible en Internet: http://www.gerencie.com/el-informe-coso.html Consultado: Marzo de 2013

CASTREJÓN, Lilian. Técnicas de Auditoria. Disponible en internet: http://www.gestiopolis.com/recursos/documentos/fulldocs/fin1/tecaudito.htm Consultado: Abril de 2013

Clavijo, Lina maría. Auditoría General y Control Interno. Disponible en internet: http://auditoriaycontrol2010b.blogspot.com/2010/08/definicion-generica-de-auditoria.html Consultado: Abril de 2013

Conceptos Universales de Auditoría. Elaboración de los Programas de Auditoria. Disponible en internet: http://fccea.unicauca.edu.co/old/tgarf/tgarfse67.html Consultado: Marzo de 2013

DARTHSOUL. Cobit4.1. Disponible en Internet: http://www.chullohack.com/2009/07/31/cobit-4-1-en-espanol/ Consultado: Marzo de 2013

ICONTEC. Reglamento del Servicio de Normalización Nacional. Disponible en Internet:http://www.icontec.org.co/files/reglamento_de_normalizacion.pdf Consultado: Marzo de 2013

MANSO, Gerónimo. Etapas de una Auditoría de Sistemas. Disponible en Internet: http://www.geronet.com.ar/?p=48 Consultado: Marzo de 2013

Naranjo, Alicia. Objetivos Generales de una auditoria de sistemas. Disponible en internet: http://anaranjo.galeon.com/objetiv_audi.htm Consultado: Abril de 2013

SALAZAR, Hernández. Trazas y Huellas. Disponibles en Internet:http://www.angelfire.com/tx/rolas/audi/clase18_19feb_traza_softevi.htm Consultado: Marzo de 2013

SISTEMAS Y ASESORÍAS DE COLOMBIA S.A. Información del sistema de dinámica gerencial hospitalaria (DGH) [en línea]. http://www.syac.com.co/producto3.aspx

UNIPAMPLONA. Planeación Estratégica de los Sistemas de Información. Disponible en internet:

https://docs.google.com/document/d/1RrIAiiAB0p46X9PPAF4iDVa97ZxGnZRxoUkwrF2UBtw/edit?pli=1 Consultado: Abril de 2013

http://www.hosdenar.gov.co

ANEXOS

Los anexos relacionados a continuación se entregan por medio magnético y se adjuntan al presente informe.

ANEXO1.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –PO2. Definición de la arquitectura de información.

ANEXO2.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –PO3. Determinar la dirección tecnológica.

ANEXO3.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –PO7. Administrar recursos humanos de TI.

ANEXO4.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –PO9. Evaluar y administrar los riesgos de TI.

ANEXO5.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –AI3. Adquirir y mantener infraestructura tecnológica.

ANEXO6.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –AI7. Instalar y acreditar soluciones y cambios.

ANEXO7.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –DS5. Garantizar la Seguridad de los Sistemas.

ANEXO8.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –DS12. Administrar el ambiente físico.

ANEXO9.Cuadros de Definición de Fuentes de Conocimiento, pruebas de análisis y pruebas de auditoría –ME2. Monitorear y evaluar el control interno.

ANEXO10.Cuestionario cuantitativo –PO2. Definición de la arquitectura de información.

ANEXO11.Cuestionario cuantitativo –PO3. Determinar la dirección tecnológica.