UNIVERSIDAD DEL BIO-BIO

FACULTAD DE CIENCIAS EMPRESARIALES

DEPARTAMENTO DE GESTION EMPRESARIAL

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

Y TECNOLOGIAS DE INFORMACION

AUDITORÍA INFORMÁTICA A LA SECCIÓN DE ABASTECIMIENTO DEL HOSPITAL CLÍNICO HERMINDA MARTÍN DE LA CIUDAD DE CHILLÁN

Julio César Contreras Jeldres

Cristian Alejandro Chandía Poblete

Profesor Guía: Alfonso Rodríguez Ríos

Agradecimientos

Al finalizar el proyecto de titulación quisiera expresar mi mayor gratitud a mi familia la cual permaneció siempre presente en esta compleja y satisfactoria etapa de mi vida, brindando completo apoyo en los momentos difíciles y festejando los logros alcanzados.

Además agradezco a los amigos que pude conocer en estos años de carrera, a los que ya salieron y los que quedan.

Con amor agradezco a Silvia, por no permitirme decaer e impulsarme a alcanzar mis objetivos.

Gracias a todos ellos por ayudarme a crecer como persona y como profesional.

Cristian Chandía Poblete

Agradecimientos

Al concluir esta larga etapa de mi vida, no me queda más que agradecer por todo el apoyo, motivación y paciencia entregada por mi familia, durante estos 9 años de Universidad.

Además agradezco por todos los amigos y lugares de larga franja de tierra que pude conocer gracias a mi Universidad.

Gracias a todos los profesores, amigos, auxiliares y secretarias por ayudarme a crecer como persona y como profesional.

No puedo finalizar estos agradecimientos sin antes recordar a todos los compañeros caídos en la dura batalla universitaria.

Se despide sin otro particular.

Julio César Contreras Jeldres.

Resumen

La Sección de Abastecimiento del Hospital Clínico Herminda Martin de la ciudad de Chillan, es una Unidad dependiente del Subdepartamento de Abastecimiento y Finanzas, cuyo objetivo es el de adquirir, recepcionar, almacenar y distribuir todos los insumos utilizados por el Hospital, tanto en su labor clínica como administrativa.

La Sección de Abastecimiento utiliza para dar cumplimiento a sus funciones el Modulo Abastecimiento Sur del Sistema de Información base del Hospital denominado ANITA. Este sistema fue desarrollado por la Empresa IBM a mediados de los noventa, cumpliendo con los requisitos principales de al época. En la actualidad los requisitos han cambiado y es necesario analizar si los Sistemas de Información dan cumplimiento a ellos. Además se hace uso del Sistema de Costos HERMINDA.

Los procedimientos de compra, recepción, despacho de la Sección de Abastecimiento son fundamentales para el funcionamiento del Hospital por lo que su correcta ejecución garantiza la entrega de un buen servicio. Tanto en la ejecución de los procedimientos, como la utilización de los Sistemas de Información la Sección de Abastecimiento interactúa con otras unidades del Hospital, por lo cual el área de investigación se amplia específicamente a la Oficina de Ingeniería de Sistemas y el Área de Soporte de Comunicaciones.

La Subdirección del Hospital Clínico Herminda Martín requiere contar con información actualizada del estado actual de la Sección de Abastecimiento, relacionado con los Sistemas de Información, procedimientos y seguridad. Buscando estos objetivos es que se ha decidido realizar como proyecto de titulo una Auditoria Informática a la Sección de Abastecimiento. La cual recopilara información relevante como evidencia que sustente la opinión del Equipo Auditor.

Para determinar el nivel de cumplimiento de la Sección se determino junto al Jefe de la Sección de Abastecimiento los objetivos generales de la Auditoria, que apuntaban a temáticas relevantes para la dirección. Con los objetivos determinados se adapto la Auditoria se desarrollo adaptando la metodología sugerida por Mario Piattini en su libro “Auditoria Informática Un Enfoque Practico”, se han utilizado técnicas como cuestionarios,

entrevistas, revisión de documentación, observación. La información obtenida se sometió a un proceso de análisis y evaluación, producto de aquello se logro obtener el estado actual de la Sección en relación a los objetivos iniciales que fueron planteados.

El informe de Auditoria entrega la opinión del Equipo Auditor y el sustento de la misma. Aportando además sugerencias que permitan la mejora de los aspectos críticos encontrados.

El Equipo Auditor espera que los objetivos de la Subdirección del Hospital se hayan cumplido mayoritariamente, y que la información recavada sea de utilidad para la Institución.

INDICE

INTRODUCCIÓN

Salvaguardar los activos que posee una organización es piedra angular de las acciones que rigen a los directivos, entre ellos puede destacar activos tales como la información, sistemas de información desarrollados o comprados, equipamiento computacional, el recurso humano que lo conforma, y los clientes fieles a los servicios brindados. En el presente caso de estudio este principio logra alcanzar relevancia absoluta, debido a que la organización brinda servicio de salud a la comunidad y los clientes pierden su calidad de simples consumidores, transformándose en pacientes que requieren obtener una atención integral y satisfactoria de sus necesidades de salud. Cambiando el enfoque de una empresa que busca la rentabilidad económica como principio base de sus operaciones, a una institución sin fines de lucro que busca el bienestar de la comunidad.

La Sección de Abastecimiento y bodega del Hospital Clínico Herminda Martín de la Ciudad de Chillán (HCHM), dependiente de la Subdirección Administrativa, es una unidad elemental de la estructura organizativa, puesto que ella tiene como labor el abastecimiento a las diversas unidades del establecimiento, de tal manera que estás puedan brindar un servicio eficiente tantos en las labores internas como hacia la comunidad, agregando a su misión la búsqueda permanente de la optimización de los recursos públicos asignados al establecimiento.

Mayoritariamente los procesos que comprende la ejecución de las labores de la sección son gobernados por sistemas de información que se encuentran automatizados, los cuales brindan apoyo y son el soporte para el resguardo seguro de la información que es obtenida y manipulada por el personal. Estos sistemas de información son de administración diversa, algunos dependientes de la Oficina de Ingeniería de Sistemas, como lo es el Sistema IBM, y otros que recae su administración en personeros públicos externos como es el portal Mercado Público.

Persiguiendo el cabal cumplimientos de los objetivos de la Sección de Abastecimiento y bodega, es que se ha planteado el desarrollo de un proceso de Auditoría Informática a los sistemas que gobiernan las actividades de la Sección de Abastecimiento.

El Equipo Auditor que desarrolló las actividades que comprende el proceso, esta conformado por alumnos de las Carreras de Ingeniería de Ejecución en Computación e Informática y Contador Público y Auditor de la Universidad del Bio Bío que en modalidad de proyecto de título, han llevado a cabo este estudio consolidando la amplia formación académica, con una opinión más en profundidad y con un sustento mayor.

En decisión acordada por el Equipo Auditor, se amplió el espectro de evaluación del proceso de auditoría, abordando temáticas como la Seguridad Física y Lógica, los procesos fundamentales que comprenden la labor de la Sección de Abastecimiento. La evaluación comprendió además la indagación de la información proveniente de otras secciones, como son la Oficina de Ingeniería de Sistemas y el Área de Soporte de Comunicaciones, los cuales brindan servicios que sustentan los procesos de abastecimiento y además de la labor propia desempeñada, como es la administración de los sistemas de información y el mantenimiento del equipo computacional.

La decisión de incluir las temáticas mencionadas se sustenta en los principios que fundamentan la presente auditoría, que es brindar una opinión independiente, veraz, y que entregue información relevante del estado actual de la sección, aportando a la toma de futuras decisiones por parte de la administración.

El documento elaborado cuenta con cuatro capítulos y una serie de anexos que complementan la información obtenida y la evaluación efectuada, el contenido general de cada capítulo se detalla a continuación:

Capítulo I, Marco Teórico; Comprende el sustento del proceso realizado, indicando definiciones relevantes de aspectos claves que deben ser conocidas. Se plantea

además los objetivos que se buscan en ese proceso de Auditoría Informática, las técnicas, herramientas y fuentes que el equipo auditor utilizó.

Capítulo II, Planeación de la Auditoría; Comprende la interiorización de la sección sujeta a evaluación, su estructura organizacional, funciones principales, actividades del personal que la compone. Se enfatiza en los procedimientos primordiales que comprenden la labor de la sección, detallando las actividades que allí se llevan a cabo.

En el presente capítulo se profundiza en los sistemas de información que gobiernan los procedimientos claves de la sección y sus características, como interfaces de usuario, operaciones. Estos sistemas de información son; Sistema IBM Modulo ABASUR (ANITA[1]), Sistema de Costos HERMINDA, Portal Chile Compras.

El capítulo comprende además, los objetivos, alcance, oportunidad, planeación de la auditoría, la metodología utilizada y el detalle de los controles puestos a prueba.

Capítulo III, Ejecución de la Auditoría; Comprende la evaluación de los controles efectuados y el análisis de riesgos. Se indica que este capítulo y sus anexos correspondientes son el sustento o evidencia de la opinión vertida en el informe de auditoría.

Capítulo IV, Informe de Auditoría; Comprende la elaboración del documento considerado como más relevante de todo el proceso de autoría.[2]

En el capítulo se emite la opinión del equipo auditor, la evidencia que lo sustenta y las sugerencias propuestas.

[1] Denominación que recibe el Sistema de Información base del Hospital que integra diferentes módulos como; Abastecimiento, Finanzas, Atención Médica y Farmacia.

[2] José de la Peña Sánchez, Auditoría Informática Un Enfoque Práctico, Capítulo 4, Página 100, Año 200.

CAPÍTULO I - MARCO TEÓRICO

1.1. La Auditoría Informática

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información resguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos[3].

El objetivo principal de una Auditoría Informática es comprobar la fiabilidad de la herramienta informática y la utilización que se hace de la misma[4].

Debido a la complejidad que surge en el entorno informático y de los procesos que en ella se ejecutan, es realmente difícil alcanzar aquel objetivo, aun cuando un sistema de información sea aparentemente de fiabilidad total, puede ocultar a su vez grandes vacíos. Lo mismo puede suceder de forma inversa, por lo cual aun cuando se cuente con una gran experiencia es difícil para el auditor informático tener la seguridad de la fiabilidad total en este entorno.

La Auditoría Informática no puede ser exacta en cuanto a la fiabilidad del software, pero si puede dar opiniones fundadas y serias sobre la fiabilidad del entorno informático. Además puede comprobar que el entorno informático aplique las políticas de la dirección, se rija por normas establecidas y cumpla de manera eficiente sus funciones.

La Auditoría Informática es útil, pero se debe tener presente que no es una ciencia exacta, pues debe apoyarse en una serie de suposiciones bien fundadas. Es por estas razones por la cual los objetivos asignados a una Auditoría Informática, las técnicas y herramientas son variables[5].

1.1.1. Funciones a desempeñar en la Auditoría Informática

Las funciones que un Equipo Auditor Informático puede desempeñar en una organización, se pueden agrupar en tres grupos:

[3] Gloria Sánchez Valriberas, Auditoría Informática un Enfoque Práctico, Capítulo 2, Página 28, Año 2001.
[4] Yann Derrien, Técnicas de la Auditoría Informática, Página 5
[5] Yann Derrien, Técnicas de la Auditoría Informática, Página 7

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases de cambio.
- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las normativas implantadas por la dirección, requisitos legales, protección de confidencialidad y protección ante errores, pérdidas y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

La memoria de título a desarrollar denominada "Auditoría Informática a la Sección de Abastecimiento del Hospital Clínico Herminia Martín de la Ciudad de Chillán" se enfocará en dar cumplimiento a los dos grupos finales de funcionalidades, verificando los sistemas de información existente, además de la implantación de controles de seguridad y correcto cumplimientos con los procedimientos establecidos.

1.1.2. Los Objetivos del Proyecto de Auditoría Informática

El objetivo del presente proyecto es realizar una Auditoría Informática externa en la cual se emitirá una opinión independiente y profesional, relacionado con la calidad de los sistemas de información que gobiernan la Sección de Abastecimiento del HCHM y del uso que de ellos se hace. Sumado a esto se analizaran el área verificando que los procedimientos y políticas provenientes de la dirección se realicen adecuadamente. Adicionalmente se analizará el área desde el punto de vista de la seguridad física y lógica.

Considerando que la Sección de Abastecimiento es un usuario de los sistemas que lo gobiernan y el control de los sistemas depende del área de Informática, el estudio comprenderá el conocimiento en profundidad de ambas áreas, considerando procedimientos, políticas, equipamiento computacional, manuales, sistemas de información entre muchos otros elementos que los componen.

1.1.3. Fuentes de la Auditoría

El Equipo Auditor debe tener claro cuales serán las fuentes que le permitan obtener la información para el desarrollo del proceso de auditoría, la cual debe estar disponible durante todo el proceso. Algunas fuentes a utilizar en el proyecto serán:

- Políticas, Normas y planes de seguridad que provengan de la organización, como del área auditada.
- Auditorías anteriores, de carácter general o específico, que de alguna manera se relacionen con el área a auditar.
- Entrevistas con el personal administrativo, de informática, de seguridad y de otras actividades relevantes para el área.
- Planes de Contingencia.
- Informes sobre acceso y visitas.
- Informes sobre fallas reales producidas.
- Manuales de procedimientos para: la adquisición de productos, la recepción de productos, la distribución de productos y registro de insumos clínicos y generales.
- Informes de inventario, mermas y robos.
- Políticas de respaldo de archivos y recuperación de soportes.
- Documentación de los Sistemas de Información.
- Organigrama y descripción de Funciones.
- Archivos computacionales utilizados en los procedimientos que la sección realiza.

1.1.4. Procesos orientados del marco de trabajo COBIT.

COBIT define las actividades de Tecnologías de Información (TI) en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. El marco de

trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

Planear y Organizar (PO): Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda 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. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica.

Adquirir e Implementar (AI): Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración 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.

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 operacionales.

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.

Debido a la naturaleza de auditoría a realizar, donde se analizaran un conjunto de sistemas y procedimientos que ya se encuentran implementados en un área del HCHM, se a decidido someter a evaluación bajo el dominio de **Entregar y Dar Soporte (DS)**, el cual nos entrega un conjunto de objetivos de control de alto nivel, los que se detallan a continuación:

DS1 Definir y administrar niveles de servicio.

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los participantes sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.

DS2 Administrar los servicios de terceros.

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

DS3 Administrar el desempeño y la capacidad.

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso

brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.

DS4 Garantizar la continuidad del servicio.

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

DS5 Garantizar la seguridad de los sistemas.

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad

DS6 Identificar y asignar costos.

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

DS7 Educar y entrenar a los usuarios.

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

DS8 Administrar la mesa de servicio y los incidentes.

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

DS9 Administrar la configuración.

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

DS10 Administración de problemas.

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El

proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.

DS11 Administración de datos.

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

DS12 Administración del ambiente físico.

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

DS13 Administración de operaciones.

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

1.1.5. Técnicas y Herramientas a Utilizar

Las técnicas y herramientas facilitan al Equipo Auditor la obtención de evidencia que pueda sustentar la opinión emitida.

Técnicas

Algunas técnicas que serán utilizadas en el proyecto serán:

- **Observación** de las instalaciones del área, sistemas de información, procedimientos realizados, cumplimiento de normas, cumplimiento de responsabilidades. Esta técnica implica la participación como espectador o actor directo en los procedimientos mencionados.
- **Entrevistas** al personal administrativo, del Sección de Abastecimiento, al personal del área de desarrollo y soporte informático, de bodegas clínicas y bodega general, al personal de la unidad de compra y al personal que se relacione de forma directa con el área a auditada.
- **Listas de Comprobación (Checklist)** que permiten verificar que lo que se dice que se hace efectivamente se realice. Se registra de forma afirmativa o negativa si un punto a evaluar se esta cumpliendo.
- **Pruebas de Sustantivas o de Validación,** orientadas a detectar la presencia o ausencia de errores o irregularidades en los procesos, actividades, transacciones o controles internos integrados en ellos[6].

Herramientas

Las herramientas permiten respaldar la información obtenida de forma permanente, pero su uso debe ser discreto, y con el consentimiento del personal.
En el proyecto a realizar se utilizarán las siguientes herramientas:

- Grabadora de Audio
- Cámara Fotográfica

[6] José María Madurga Oteiza, Auditoría Informática Un Enfoque Práctico, Capítulo 19, Página 453, Año 2001.

- Cámara de Video
- Cuaderno de Notas

1.1.6. Fases de la Auditoría Según EDPAA (Electronic Data Processing Auditors Association)

La EDPAA, que en 1993 pasó a llamarse ISACA[7] (Information Systems Audit and Control Association) ha desarrollado una serie de fases que comprenden el ciclo de vida de la auditoría, no especificando el tipo de auditoría a la cual debe aplicarse, por lo cual se ha tomado como guía para el proyecto de auditoría informática a efectuar, estas fases son:

Fase 1: Alcance de la Auditoría

Fase 2: Adquisición de Información General de la Organización

Fase 3: Administración y Planificación

Fase 4: Plan de Auditoría

Fase 5: Resultado de las Pruebas

Fase 6: Conclusiones y Comentarios

Fase 7: Borrador del Informe

Fase 8: Discusión con los Responsables de Área Auditada

Fase 9: Informe Final (Contiene el Informe, Anexos del Informe, Evidencias)

1.2. Seguridad Física

La seguridad física presente en área es un de los objetivos del Proyecto de Auditoría a desarrollar.

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un centro de procesamiento de datos.

Si se comprende la posibilidad de la existencia de un riesgo de falla, sea esta de carácter local o general, se deberán considerar tres medidas para lograr mitigar el impacto

[7] http://www.isaca.org/

que la manifestación de los riesgos acarrearán a la organización. Estas medidas son implementadas de acuerdo a un orden cronológico, siendo medidas que se tomen[8]:

- **Antes**

  Las medidas que se tomen antes buscan obtener y mantener un nivel adecuado de seguridad física sobre los activos.

  Ejemplo de estos son; la ubicación del centro de procesamiento de datos, potencia eléctrica, control de accesos, sistemas contra incendios, medidas de seguridad, entre otros.

- **Durante**

  Las medidas dispuestas durante fallas o desastre buscan la ejecución adecuada del plan de contingencia.

  Se deben contar con los medios necesarios que permitan afrontar los fallos que puedan producirse y poder volver a operar normalmente a la brevedad posible.

  Ejemplos de estas medidas son; realizar un análisis de riesgos de sistemas críticos, establecer un tiempo límite en que las operaciones deben ser reanudadas antes de sufrir pérdidas, asegurar la capacidad de las comunicaciones, asegurar la capacidad de los respaldos.

- **Después**

  Las medidas dispuestas para después, tienen el objetivo de lograr compensar las pérdidas, gastos producidos en el centro de procesamiento de datos una vez detectado y corregido los fallos.

  Ejemplos de estas medidas son; seguros para centro de procesamiento de datos y equipamiento, seguros por interrupción del negocio que cubren pérdidas causadas por la caída de los sistemas o fallas en los

[8] Gabriel Desmonts Basilio, Auditoría Informática Un Enfoque Práctico, Capítulo 8, Páginas 182-185, Año 2001.

equipamientos computacionales, seguros para el transporte de medios protegiéndolos ante pérdidas o daños.

1.2.1. Áreas de la Seguridad Física

De acuerdo a lo expuesto por Gabriel Desmonts[9] en relación con las áreas de incumbencia directa del auditor informático, hemos extraído las que a nuestro juicio formarán parte del proceso de auditoría a realizar, estas son:

- **Centro de Procesamiento de Datos e Instalaciones**

  Se analizará el lugar físico donde se encuentra emplazado el centro de procesamiento de datos.

  Además se verificará que las instalaciones ayuden a llevar a cabo las funciones de informáticas, proporcionando seguridad a las personas, software y materiales.

- **Equipos y Comunicaciones**

  Son elementos que componen el centro de procesamiento de datos, como los computadores, terminales, equipos de almacenamiento, impresoras, medios de comunicación.

- **Administración de la Seguridad**

  Visión general de las funciones, dependencias, cargos y responsabilidades de los elementos que la componen como:

  - Responsable de la Seguridad Informática
  - Administradores de Red.
  - Administradores de Bases de Datos.

1.3. Seguridad Lógica

Se verificará y juzgará que cada usuario de los sistemas de información sólo pueda acceder a los recursos a los que le autorice el propietario[10]. Verificando que cumplan sus

[9] Gabriel Desmonts Basilio, Auditoría Informática Un Enfoque Práctico, Capítulo 8, Páginas 182-185, Año 2001.
[10] Miguel Ángel Ramos González, Auditoría Informática Un Enfoque Práctico, Capítulo 17, Página 402, Año 2001.

funciones y con los permisos que se le hayan atribuido, sean estos de lectura, modificación y/o borrado.

Se revisará cómo los usuarios se identifican y autentican, quiénes les han asignado los permisos, y qué ocurre cuando se producen violaciones de acceso o de mal uso de los sistemas, comprobando quién se entera, cómo, cuándo y qué se hace para solucionarlo.

Se someterá a evaluación los tipos de autenticación utilizados por la organización, siendo el más utilizado, las contraseñas, las cuales deben regirse por normas, políticas y estándares internos o externos.

1.4. El Informe de la Auditoría

El contenido del informe a entregar como parte del proceso de auditoría, debe abarcar los siguientes puntos[11].

1. Identificación del Informe: Se debe especificar el título del informe que le permita distinguirse de otros.
2. Identificación del Cliente: Se debe identificar a los destinatarios y a las personas que efectuaron el encargo de auditoría.
3. Identificación de la entidad auditada: Se debe identificar la entidad que es sujeta de auditoría.
4. Objetivos de la Auditoría Informática: Declaración de los objetivos de la auditoría que permita identificar su propósito, señalando explícitamente aquellos que no fueron cumplidos.
5. Normativas Aplicadas y Excepciones: Se debe identificar las normas legales utilizadas, así como las excepciones de uso. Se considerará en este punto la identificación de las políticas y procedimientos internos de la organización que son utilizados.
6. Alcance de la Auditoría: Se debe especificar la naturaleza y la extensión del trabajo realizado, señalando el área auditada, período del proceso de auditoría, sistemas de

[11] José de la Peña Sánchez, Auditoría Informática Un Enfoque Práctico, Capítulo 4, Página 100, Año 2001.

información sometidos a opinión. En este punto se deben indicar las limitaciones al alcance y las restricciones del auditado.

7. Conclusiones: Informe corto de Opinión, en que se deberá detallar el tipo de opinión de la auditoría, las cuales se especifican en el Capítulo IV del presente informe, correspondiente al Informe de Auditoría.
8. Resultados: Informe largo y otros informes, que se emiten cuando los requirentes necesitan contar con mayor información del proceso de auditoría, sumando a esto una mayor transparencia de lo realizado. Se especificará un informe por cada objetivo de la Auditoría Informática.
9. Informes Previos: Se debe señalar la utilización de informes de auditorias previas, de carácter especifico o general.
10. Fecha del Informe: Se debe señalar las fechas que comprendieron el periodo de auditoría informática. Precisando las fechas de inicio y conclusión del trabajo realizado
11. Identificación y Firma del Auditor: Se debe señalar claramente los responsables del proceso de auditoría.
12. Distribución del Informe. Se debe especificar quien o quienes podrán hacer uso del informe, así como los usos concretos que se le dará.

El informe final contendrá las recomendaciones que el equipo auditor ha considerado pertinentes para su implementación.

1.5. La Opinión de la Auditoría

Una vez realizado el análisis de los resultados de las evaluaciones efectuadas, se elaborará la esencia de todo proceso de auditoría, la opinión, la cual, según lo indicado por **José de la Peña Sánchez**[12], puede ser de los siguientes tipos: favorable o sin salvedades, con salvedades, desfavorable o adversa y denegada.

[12] José de la Peña Sanchez, Auditoría Informática Un Enfoque Práctico, Capítulo 4, Página 101, Año 2001.

Opinión Favorable: La opinión denominada favorable, sin salvedades o limpia, se deberá manifestar de forma clara y precisa, y es el resultado de un trabajo realizado sin limitaciones al alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.

Opinión con salvedades: Se manifiestan las salvedades cuando éstas son significativas en relación con los objetivos de auditoría, detallándose con precisión la naturaleza y razones por las que se manifiestan. Las salvedades expuestas en el informe pueden ser las siguientes:

- Limitaciones al alcance del trabajo realizado, refiriéndose a restricciones por parte del auditado.
- Incertidumbres cuyo resultado no permita una previsión razonable.
- Irregularidades significativas.
- Incumplimiento de la normativa legal y profesional.

Opinión desfavorable: Este tipo de opinión es aplicable en caso de:

- Identificación de irregularidades.
- Incumplimiento de la normativa legal y profesional, que afecten significativamente a los objetivos de la auditoría informática.

Se deberá elaborar con detalle las razones que propiciaron una opinión de este tipo.

Opinión denegada: La denegación de la opinión puede ser producto de:

- Limitaciones al alcance de auditoría
- Incertidumbres significativas que impidan al auditor formarse una opinión.
- Irregularidades.
- El incumplimiento de normativa legal y profesional.

1.6. Recomendaciones al Auditado

Uno de los aspectos relevantes a ser tratado por el equipo auditor, y que es parte de los requerimientos del auditado, es la elaboración de recomendaciones que permitan conseguir la máxima eficiencia y rentabilidad de los medios informáticos de la organización. Estas recomendaciones deben apuntar al reforzamiento de los sistemas y el estudio de soluciones idóneas, según los problemas que el proceso de auditoría fuesen detectados, siempre y cuando las soluciones que se adopten no violen la ley ni los principios éticos de las normas de deontología[13].

El auditor no debe elaborar recomendaciones que sean innecesariamente onerosas, dañinas o que generen riesgos injustificados para la organización auditada, debiendo evitar además proponer cambios que no tengan sustento científico y que no se encuentren debidamente probadas y certificadas[14].

[13] Deontología: Conjunto de reglas y principios éticas que regulan una actividad profesional
[14] José Páez Mañá, Auditoría Informática Un Enfoque Práctico, Capítulo 7, Página 156, Año 2001.

CAPÍTULO II - PLANEACIÓN DE LA AUDITORÍA A LOS SISTEMAS DE INFORMACIÓN

2.1 Introducción

En este capítulo se dará a conocer la organización en la cual se desarrollará este proyecto, cuyo objetivo general es Auditoría Informática externa en la cual se emitirá una opinión independiente y profesional. Para lo que se requiere un conocimiento acabado de los procedimientos realizados y de los sistemas de información automatizados que gobiernan estos procesos.

Una vez conocidas las funciones y principales cargos de la Sección de Abastecimiento, se identificarán los objetivos de control y las respectivas actividades de control que se deberán comprobar, para la correcta realización de la auditoría.

2.2 Descripción del Área

La Sección de Abastecimiento es la encargada de adquirir, almacenar y distribuir en forma en eficaz los insumos que son utilizados por todas las áreas del HCHM.

2.2.1. Misión

Dar Apoyo logístico a las diferentes Unidades del establecimiento, a través de la elaboración y ejecución del Plan Anual de compras y Contrataciones.

2.2.2. Visión

Abastecer oportunamente con los bienes y servicios a las diferentes Unidades del establecimiento, de tal manera que puedan cumplir sus actividades con eficiencia y eficacia, empleando racionalmente los recursos públicos.

2.2.3 Organigrama Subdirección Administrativa

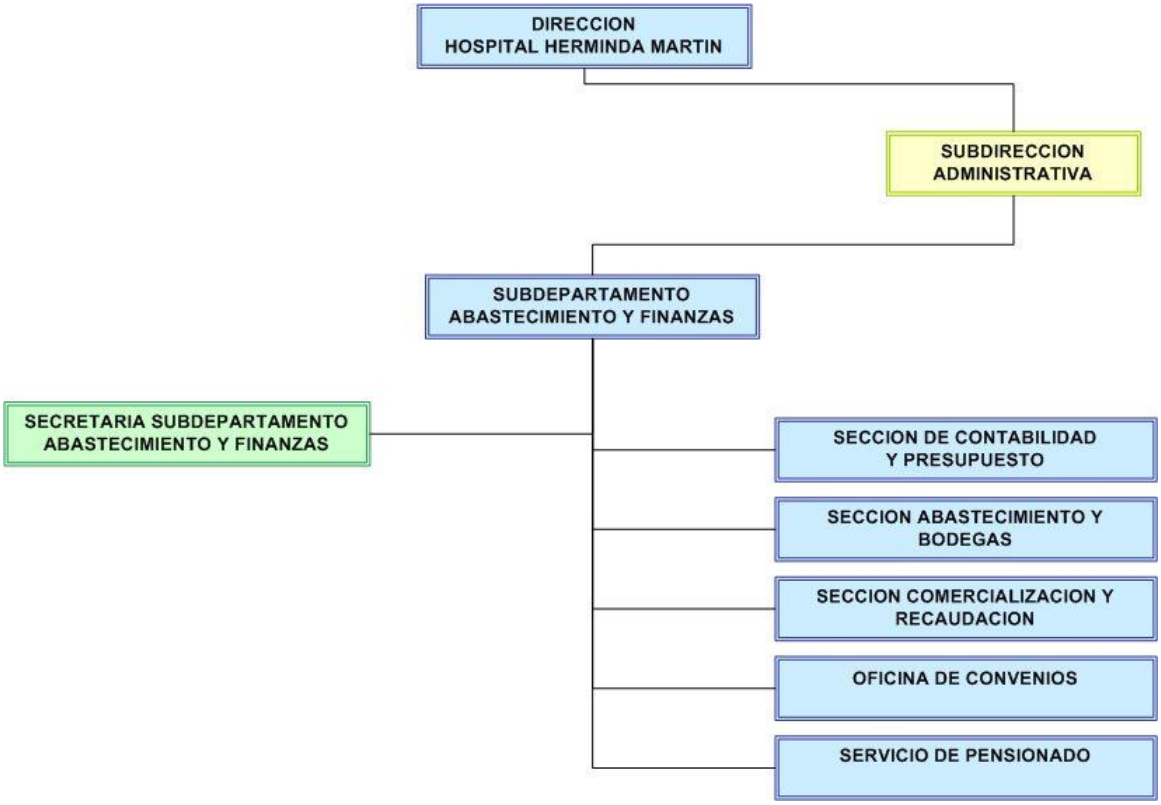

Figura 1: Organigrama Hospital Clínico Herminda Martín

2.2.4 Sección de Abastecimiento

Organigrama

La Sección de Abastecimiento se divide en tres áreas fundamentales, una correspondiente a la oficina de compras, donde se gestiona la adquisición de los insumos y dos bodegas una bodega destinada a los insumos de farmacia y una bodega para insumos generales.

Figura 2: Organigrama Sección de Abastecimiento

2.3 Descripción de cargos principales

Dentro de la Sección de Abastecimiento los cargos se encuentran definidos de manera formal y escrita, en esta descripción se indican las funciones que el personal debe realizar y las responsabilidades que estos deben asumir. A continuación se detallan los principales cargos de la sección con la finalidad de conocer las tareas que cada uno de estos debe realizar:

2.3.1. Jefe Sección Abastecimiento.

Cargo del Jefe directo: Jefe Subdepartamento de Abastecimiento y Finanzas.

Función Principal: Responsable de la marcha administrativa y funcional de la Sección Abastecimiento.

Responsabilidades:

- Programar, dirigir, coordinar, supervisar y controlar todas las actividades de la sección.
- Distribuir las tareas entre el personal asignado y controlar y evaluar su ejecución.
- Cumplir y hacer cumplir las políticas y normativa general y especial en materia de abastecimiento y funcionamiento de la sección.

- Determinar las necesidades de equipos e insumos de la sección y participar en la programación de las adquisiciones de estos elementos.
- Prestar su asesoría y colaboración técnica al Subdirector Administrativo, al Jefe del Subdepartamento de Abastecimiento y Finanzas y a otras jefaturas y dependencias del establecimiento, y cooperar en las actividades de capacitación y perfeccionamiento del personal.
- Estudiar y proponer la aplicación de nuevos sistemas y procedimientos de trabajo.

Principales Funciones

- Participar y coordinar la elaboración de los programas anuales de compras, basándose en los antecedentes visados y entregados por el Subdirector Administrativo y Jefe del Subdepartamento de Abastecimiento y Finanzas.
- Fiscalizar la preparación de las bases y demás antecedentes para efectuar los llamados a propuestas de las adquisiciones a realizar por el establecimiento, cuando corresponda, requiriendo la asesoría técnica necesaria.
- Consolidar, emitir y ejecutar los Programas de adquisiciones a realizar por el establecimiento aprobados por el Director.
- Establecer y operativizar eficientemente la relación comercial (externa), con los proveedores e instituciones que abastecen al establecimiento.
- Tramitar la suscripción de contratos de proveeduría de las áreas que no se encuentran centralizadas a través de la unidad de compras centralizadas, dependiente del Servicio de Salud Ñuble.
- Reunir y mantener información actualizada relativa a volúmenes y tendencias de consumo, existencias mínimas y máximas, tendencia del mercado e informaciones al respecto de otros establecimientos y todo otro antecedente útil para programar y efectuar las adquisiciones.
- Fiscalizar la realización de los controles de existencia, estado y calidad de los bienes e insumos del establecimiento, así como también hacer cumplir la normativa vigente sobre los procesos que ejecuta la Unidad de Bodega General, Unidad de Bodega de Farmacia y Unidad de compras.

2.3.2. Encargado oficina de compras.

Cargo del Jefe directo: Jefe Sección Abastecimiento.

Función Principal: Responsable de la marcha administrativa y funcional de la oficina de compras.

Responsabilidades:

- Responsable de la correcta y oportuna ejecución de las actividades de adquisición programadas y no programadas autorizadas por el Jefe de la Sección Abastecimiento, lo anterior en estricto cumplimiento de la Normativa vigente.
- Responsable de coordinar y supervisar la correcta ejecución de las labores propias de los funcionarios Administrativos de su dependencia.
- Responsable de supervisar que sean informadas mensualmente al Portal Chile Compra las adquisiciones efectuadas por el establecimiento, mediante la emisión de la orden de compra a través de dicho portal.
- Responsable de mantener registros estadísticos de los procesos efectuados por la oficina de compras, poniendo especial énfasis en: órdenes de compra a través del sistema ANITA, órdenes de compra a través del Portal Chile Compra, ajustes a las órdenes de compra, comportamiento de proveedores, estado de los procesos de compra.
- Responsable de la Mantención en forma ordenada y clasificada de los archivos de documentos generados en la oficina de Compras.
- Responsable de mantener en forma ordenada, clara y accesible toda la documentación generada en la oficina de compras, debiendo mantener registros únicos, y ordenados de acuerdo a criterios específicos, manteniendo siempre el correlativo de la documentación.
- Responsable de coordinar en forma trimestral, que se ejecute el proceso de anulación de Órdenes de Compra que se encuentre en el sistema “ANITA”. aún en “estado 4”, es decir, enviadas sin recepción, y cuya data supere los 60 días, situación que deberá ser coordinada con Unidad de Facturación, a fin

de evitar anulación de compromisos Presupuestarios asociados a Facturas pendientes de regularización (Notas de Crédito, Notas de Débito etc.)

- Responsable de disponer las actividades diarias al personal de la Unidad, acorde a las circunstancias y necesidades por cargas de trabajo evidenciadas.

Principales Funciones

- Encargado de coordinar las actividades de adquisición programadas y no programadas autorizadas por el Jefe de la Sección Abastecimiento, lo anterior en estricto cumplimiento de la Normativa vigente.
- Encargado de ejecutar los procesos de adquisición en permanente coordinación con las distintas entidades técnicas del establecimiento.
- Responsable de supervisar que sean informadas mensualmente al portal ChileCompra las adquisiciones efectuadas por el establecimiento, mediante la emisión de la orden de compra a través de dicho portal.
- Responsable de efectuar al menos una reunión mensual con los funcionarios Administrativos de su dependencia, debiendo emitir acta de dicha reunión y remitirla al Jefe de la Sección Abastecimiento.
- Encargado de supervisar la correcta labor del funcionario administrativo a cargo del fondo fijo, debiendo revisar, chequear y visar las planillas y rendiciones de dichos fondos.
- Responsable de supervisar el permanente seguimiento por parte de los administrativos de compras, al despacho por parte de los Proveedores de los productos adquiridos.
- Responsable de disponer las actividades diarias al personal de la Unidad, acorde a las circunstancias y necesidades por cargas de trabajo evidenciadas, propendiendo a la polifuncionalidad en el desarrollo de éstas y de conformidad al cumplimiento de plazos establecidos para las actividades que internamente deben ejecutar los funcionarios de la Unidad indicada.

2.3.3. Encargado oficina de Bodega (Farmacia y General)

Función Principal: Responsable de la marcha administrativa y funcional de la oficina de Bodegas, en el almacenamiento y distribución de productos.

Responsabilidades:

- Responsable de la marcha administrativa de la Unidad de bodega respectiva.
- Responsable del Almacenamiento y distribución de los productos a su resguardo, aplicando medidas de control y seguridad a modo de evitar mermas o pérdidas de productos.
- Responsable de la correcta preparación y procesamiento de los requerimientos de insumos y artículos necesarios de reponer o adquirir mensualmente, por parte de la Unidad de Compras de la Sección, debiendo poner a disposición de la Unidad de Compras, en forma oportuna, a más tardar los días 15 o siguiente hábil, del mes anterior al período abastecer, dichos requerimientos, los que contendrán la información de saldos y stock disponibles a esa fecha y cuyas cantidades versus valores unitarios deberán, desde ya, encuadrarse en el marco presupuestario dado para cada item respectivo. Las planillas de requerimientos de reposición de Stock de Insumos (áreas General y de Farmacia), para el siguiente mes, deberán ser remitidas a la Unidad de Compras, como se indica precedentemente, el día 15 o siguiente hábil del mes anterior al período a abastecer.
- Responsable de los procesos globales de recepción física de artículos e insumos, recepción computarizada de éstos, almacenamiento adecuado y posterior distribución a los Servicios y Unidades usuarias; velando por el cumplimiento de las medidas tendientes al mantenimiento del orden y la organización debida de las Bodegas, velando por el cumplimiento del Calendario de entregas de Pedidos.
- Responsable de la emisión, en forma oportuna, de reportes y estadísticas de consumos por Servicio, reportes de existencias físicas, reportes de existencias con baja rotación o con fecha de vencimiento próxima, productos con sobre stock y en general todo otro registro que, como herramienta de

gestión, le sea requerido por la Jefatura de la Sección y estamentos superiores.

- Responsable del control y fiscalización de la preparación y despacho, de los pedidos de insumos y artículos, materializados por medio de las planillas de Pedido Mensual o Libro de Pedido de Repaso o Urgencia que los Servicio, Secciones y Unidades usuarias formulen, poseyendo la facultad de efectuar rebajas y ajustes de cantidades, en función a stock existentes.
- Responsable de disponer las actividades diarias al personal de la Unidad, acorde a las circunstancias y necesidades por cargas de trabajo evidenciadas, propendiendo a la polifuncionalidad en el desarrollo de éstas, y de conformidad al cumplimiento de plazos establecidos para las actividades que internamente deben ejecutar los funcionarios de la unidad indicada. Deberá, paralelamente, analizar las solicitudes de Permisos Administrativos y Feriado Legal que los funcionarios de su dependencia soliciten, permisos que deberán ser autorizados por el Jefe de la Sección.
- Responsable de brindar las facilidades al personal de Sección Contabilidad y Presupuesto, en la ejecución de controles selectivos imprevistos, poniendo a disposición del personal de contabilidad los medios tendientes a facilitar los procesos de control.
- Responsable de disponer la ejecución permanente de controles y chequeos internos de stock, emitiendo el informe respectivo a la Jefatura de la Sección.
- Responsable de informar en forma oportuna a la Jefatura de la Sección, aquellos artículos cuyas cantidades físicas sean consideradas como críticas, y por tanto requieran de su reposición inmediata, y mantener una permanente comunicación y coordinación con el encargado de la unidad de compras.
- Responsable de coordinar la relación con los usuarios internos, respecto de procesos íntimamente ligados a la Unidad su cargo; especialmente con el Estamento de Enfermería, y Jefes de Departamentos y Secciones, prodigando en todo momento una adecuada y esmerada atención.

- Responsable de efectuar al menos una reunión mensual con los funcionarios Administrativos de su dependencia, debiendo emitir acta de dicha reunión y remitirla al Jefe de la Sección Abastecimiento.

2.4. Descripción de Procedimientos del área

Para el desarrollo correcto de la auditoría con una opinión fundamentada, se debe conocer en profundidad los procedimientos que se realizan dentro de la Sección de Abastecimiento, para lo cual se presentan los diagramas de procesos y la respectiva descripción de cada uno de los pasos que componen el procedimiento, estos procedimientos se encuentran documentados formalmente dentro de la Sección de Abastecimiento.

2.4.1. Procedimiento de Despacho

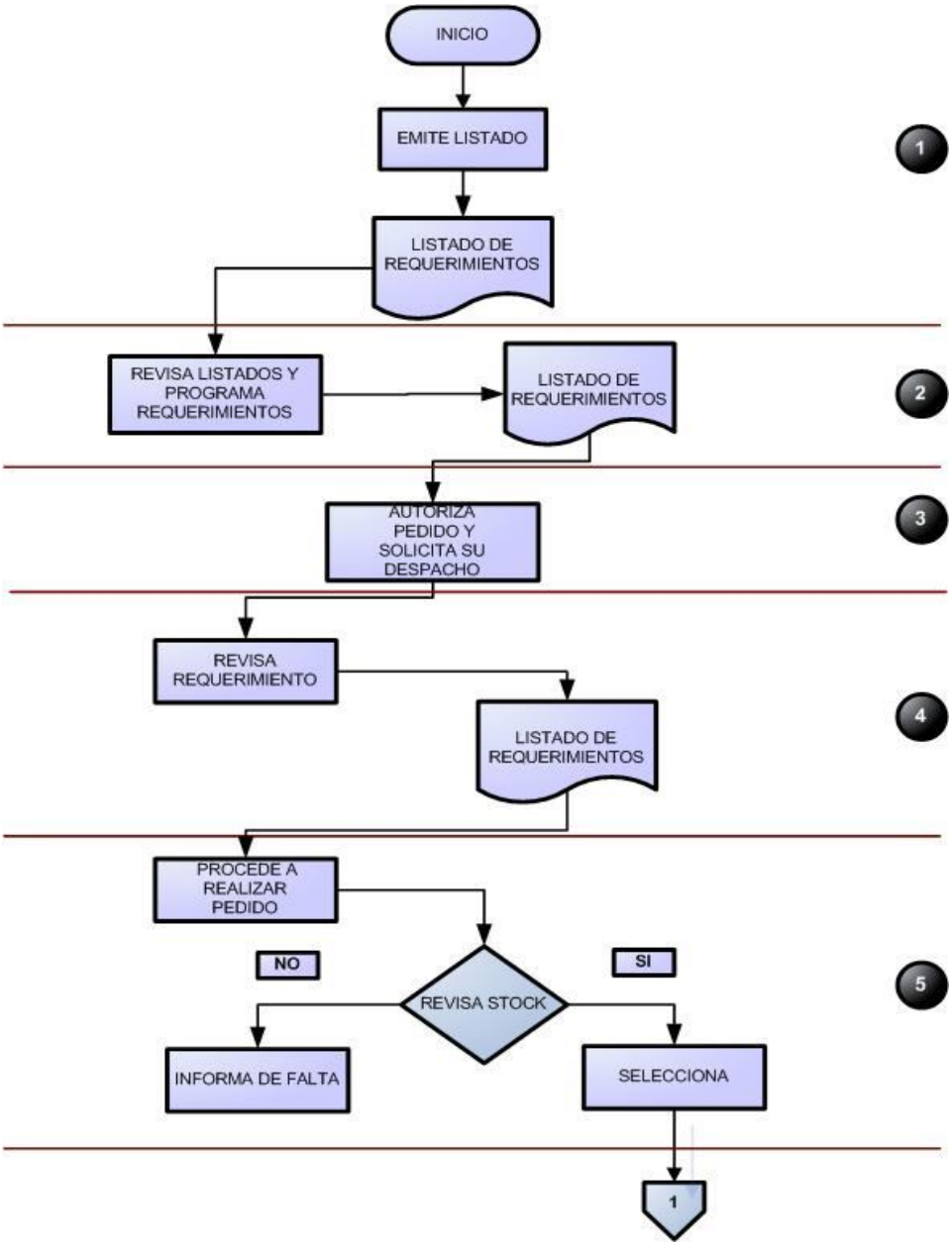

Figura 3: Procedimiento Despacho Parte 1

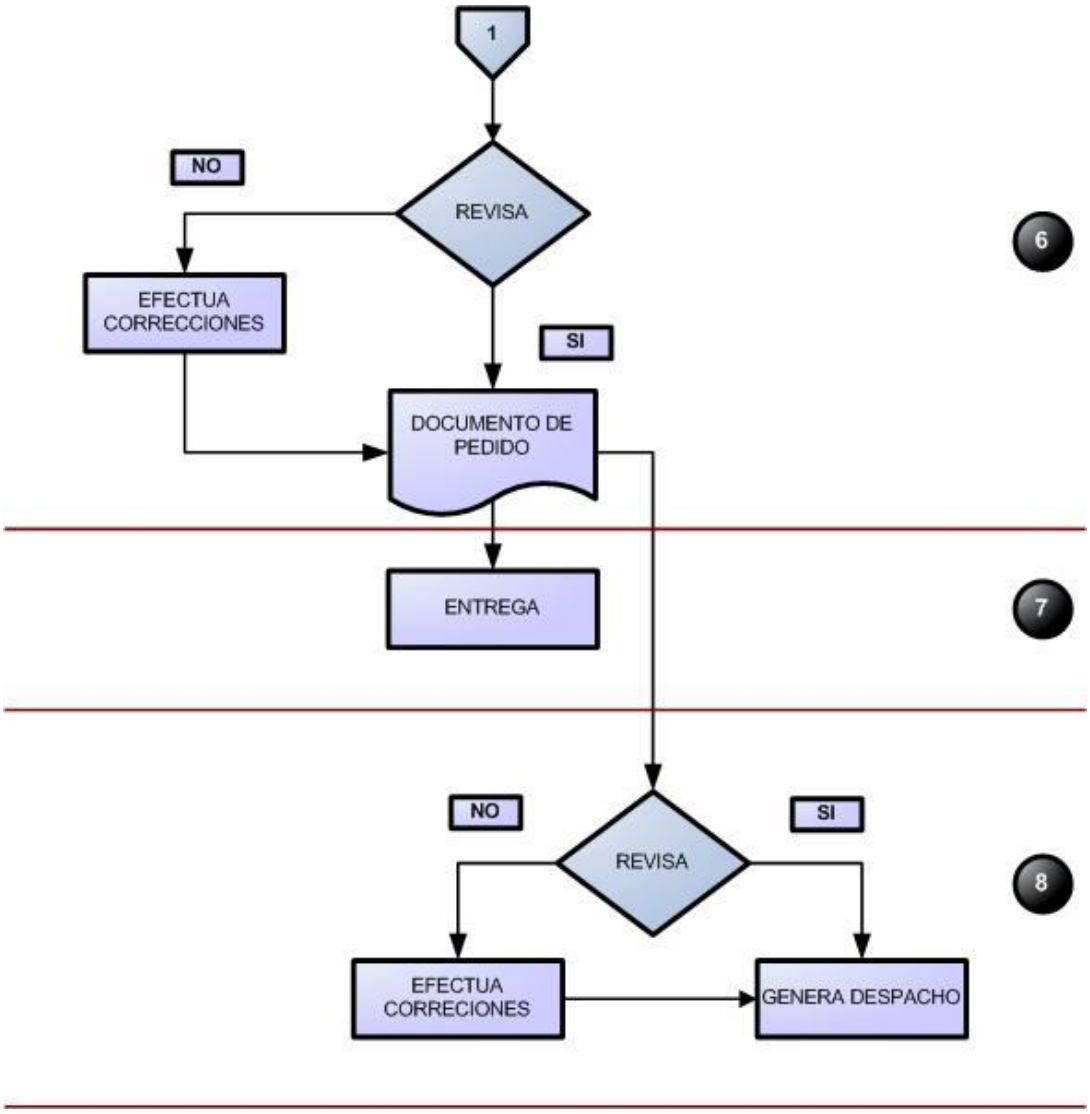

Figura 4: Procedimiento Despacho Parte 2

Descripción Procedimiento de Despacho.

El Procedimiento se lleva a cabo con la finalidad de distribuir a las diferentes unidades o servicios clínicos, los insumos que se requieren para el correcto funcionamiento del centro hospitalario. Para su registro y ejecución, el Sistema ANITA cuenta con las siguientes etapas, Solicita, Visa, Autoriza y Entrega. En su ejecución intervienen:

1. Encargado de Bodega.
2. Jefe de Unidad (Requirente).
3. Encargado de Despacho.
4. Auxiliar de Bodega.

El Procedimiento se divide en 8 pasos los cuales se detallan a continuación.

- **Paso 1:** El proceso se inicia cuando el Encargado de Despacho emite un listado de pedido en el cual se señalan los insumos disponibles, según la planificación para una unidad determinada. El listado de pedido es enviado a la unidad requirente.
- **Paso 2:** El Jefe de Unidad revisa su stock propio y en base al listado solicita los insumos necesarios para completar el stock para su funcionamiento semanal/mensual, donde se genera un listado de requerimientos que es enviado al Encargado de Bodega.
- **Paso 3:** El listado de requerimientos es revisado y autorizado por el Encargado de Bodega el cual procede a entregarlo a al Encargado de Despacho.
- **Paso 4:** El Encargado de Despacho revisa el listado y entrega al Auxiliar de Bodega.
- **Paso 5:** El Auxiliar de Bodega procede a revisar la estantería y seleccionar los productos, los cuales posteriormente son ubicados en el lugar dispuesto para la posterior revisión del Encargado de Despacho. En caso de no existir stock informa falta de productos.
- **Paso 6:** El Encargado de Despacho revisa los productos confirmando cantidad, calidad y presentación y procede a incorporar la cantidad solicitada en la hoja de pedido, ya sea en su totalidad de la cantidad solicitada o en forma parcial.
- **Paso 7:** El Auxiliar de Bodega realiza la entrega física de los productos a la unidad requirente.
- **Paso 8:** El Encargado de Despacho revisa el listado de pedido confirmando la correcta codificación y procede a registrar en proceso en el sistema ANITA.

2.4.2. Procedimiento de Recepción

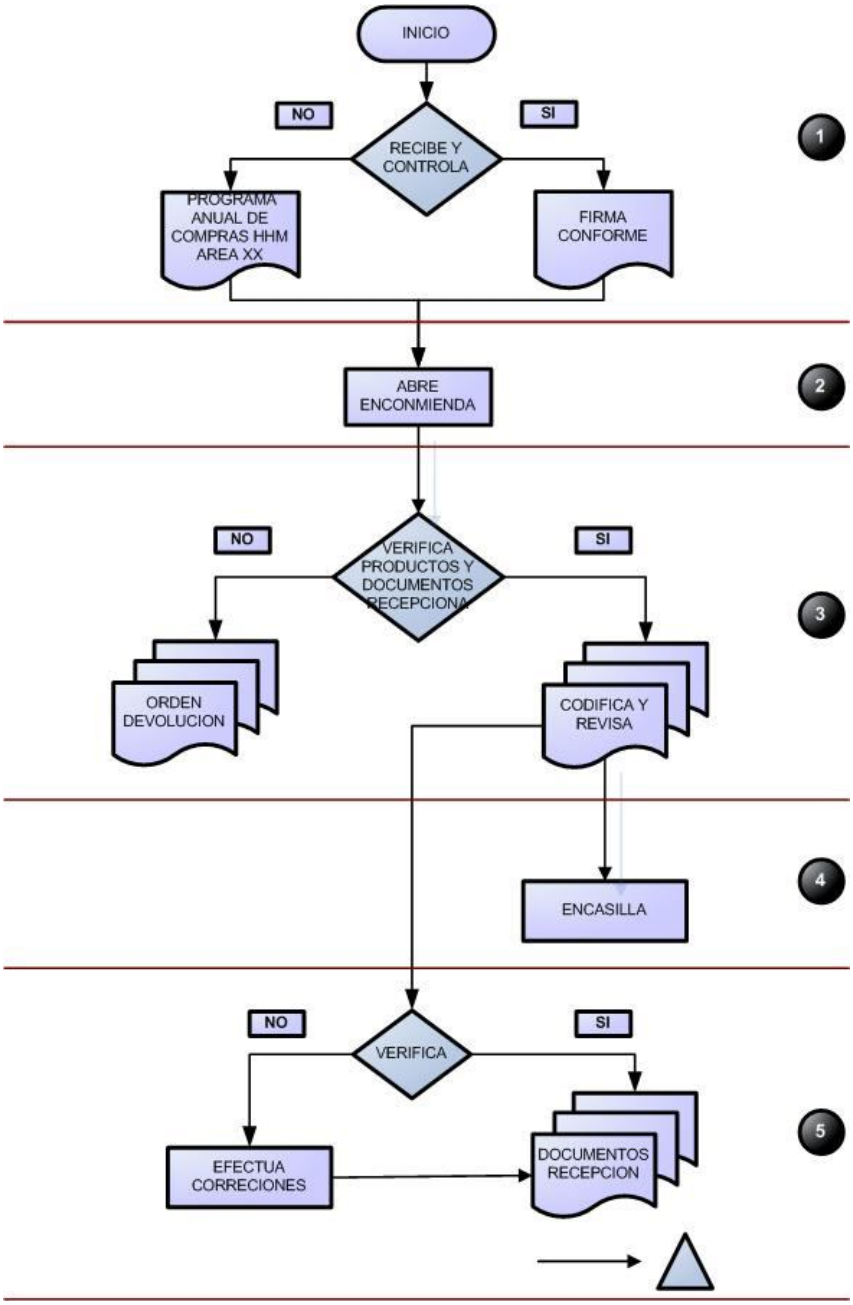

Figura 5: Procedimiento de Recepción Parte 1

Descripción Procedimiento de Recepción.

El procedimiento se lleva a cabo para recepcionar las compras realizadas a los diferentes proveedores de insumos, este procedimiento interactúa con el Sistema ANITA en el cual se codifica la información de los productos recibidos. El personal involucrado es:

1. Encargado de Recepción.
2. Auxiliar de Bodegas.

El procedimiento se divide en 5 pasos los cuales se detallan a continuación:

- **Paso 1:** El proceso se inicia cuando el Encargado de Recepción, recibe la encomienda con la mercadería y procede a contar y controlar que el número de bultos coincida con los que se indican en la papeleta de transporte, en caso que estos no coincidan se procede a generar documento de reclamo e informa al transportista de la diferencia.
- **Paso 2:** El Auxiliar de Bodegas, abre los paquetes que componen la encomienda y los ordena para su revisión.
- **Paso 3:** El Encargado de Recepción coteja la orden de compra versus la factura o guía de despacho, verificando precio, cantidad y estado de los productos. De encontrar alguna irregularidad procede a generar una orden de devolución, detallando si corresponde nota de crédito o cambio del producto, este debe incluir factura. En caso de no encontrar irregularidades el encargado de bodega procede a codificar y designar Auxiliar de Bodegas para encasillar los productos.
- **Paso 4:** El Auxiliar de Bodegas procede a encasillar los productos ya codificados en el estante correspondiente.
- **Paso 5:** Verifica información recibida en guía de despacho o factura versus orden de compra poniendo énfasis en los factores de conversión, precio y cuadratura. Si la información cotejada es correcta emite documento de recepción en triplicado entregando copia a facturación (adjuntando copia de guía o factura).

2.4.3. Procedimiento de Facturación

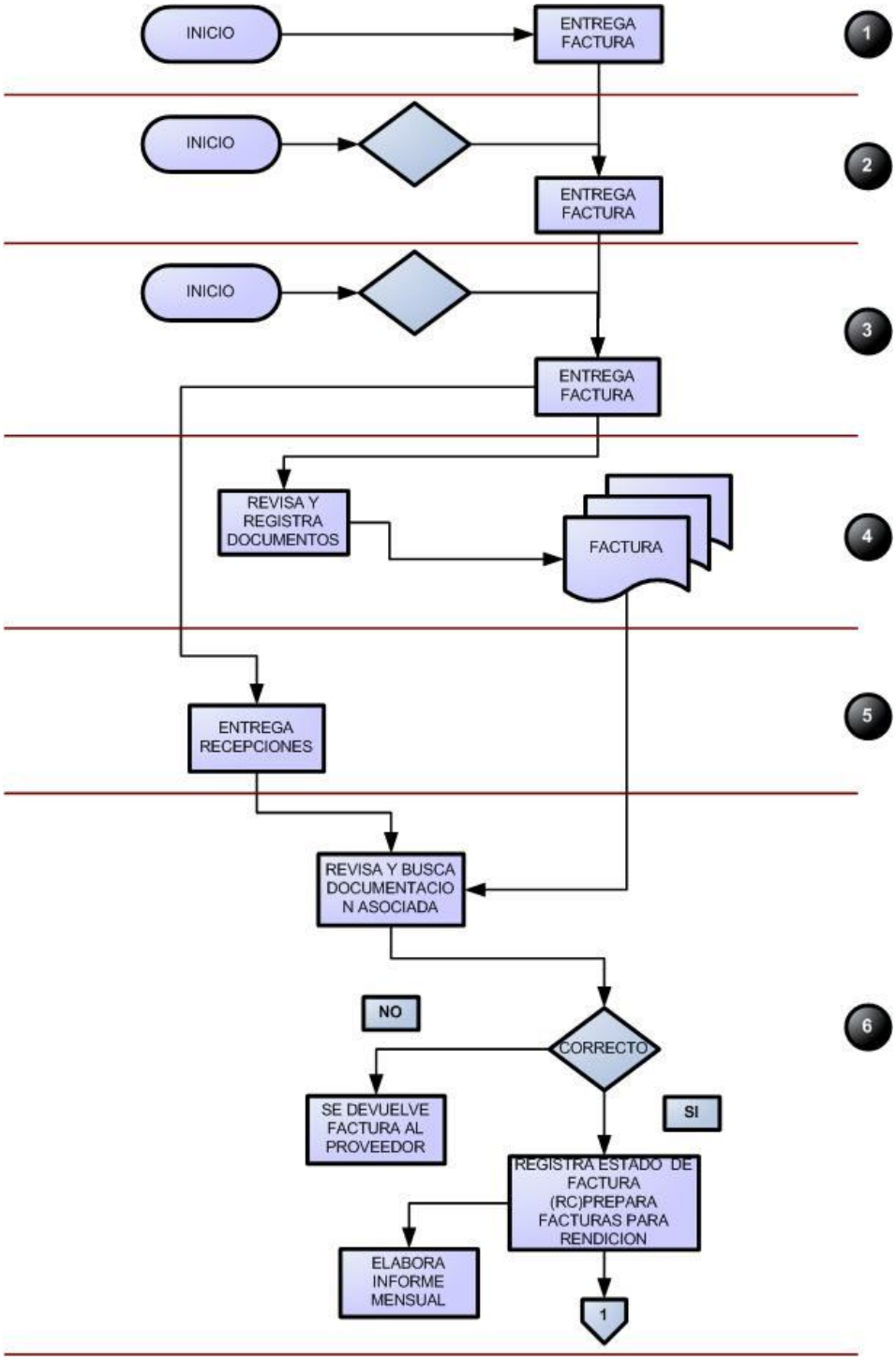

Figura 6: Procedimiento de Facturación Parte 1

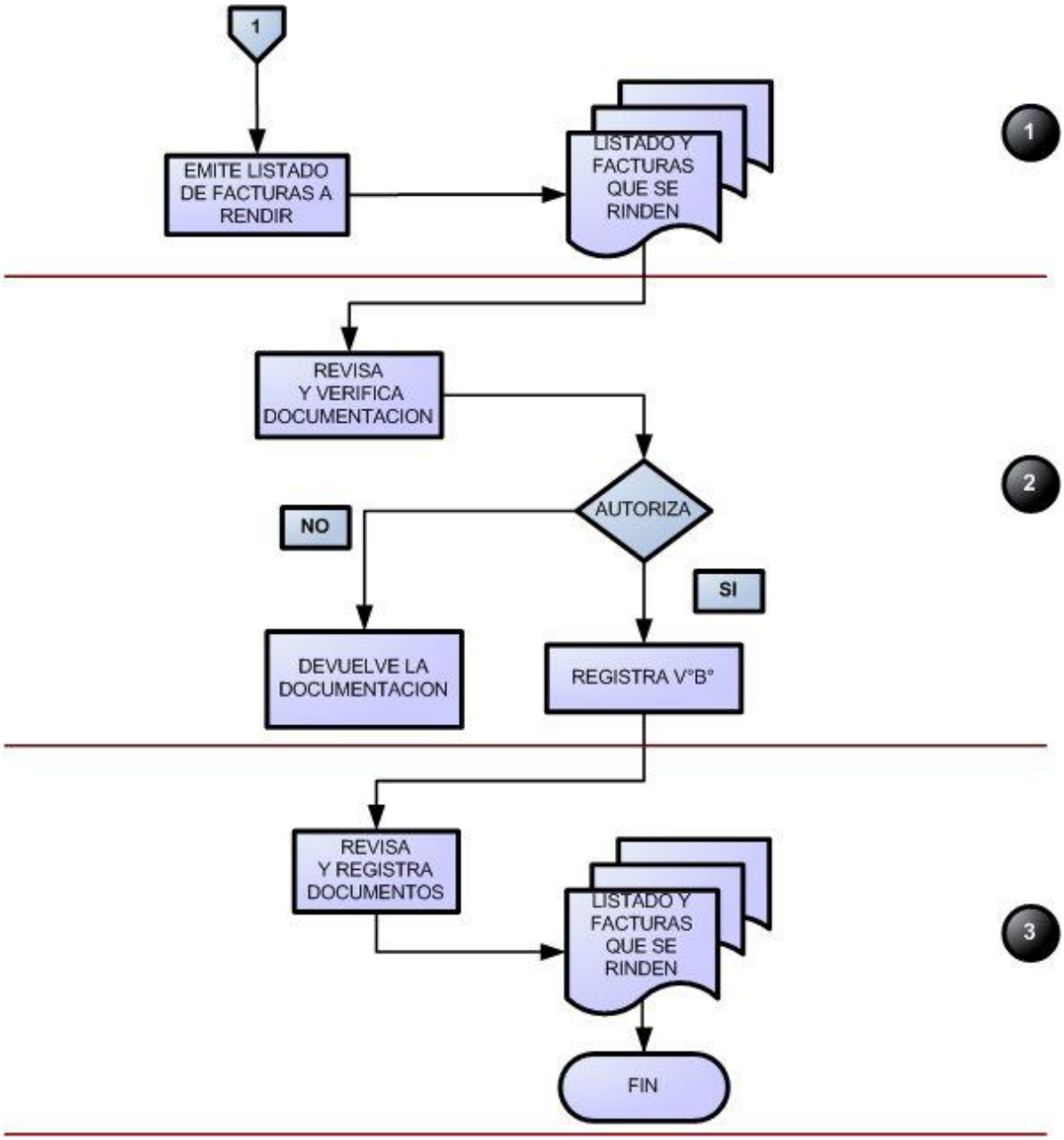

Figura 7: Procedimiento de Facturación Parte 2

Descripción Proceso de Facturación.

El objetivo de este procedimiento es registrar todas las facturas a devengar (la factura se registra aun cuando el pago o cobro no se haya efectuado). Los participantes de este proceso son los siguientes:

1. Jefes de Departamentos; SASI, SOME, Laboratorio, Computación.
2. Administrativo Oficina de Partes
3. Encargado Recepción Física de Abastecimiento.
4. Encargado de Facturación de Abastecimiento.
5. Encargado de Recepción por Sistema Abastecimiento.
6. Encargado de la Unidad de Rendición de Facturas.
7. Encargado de Control Interno de Contabilidad.
8. Encargado de Ejecución Presupuestaria.

El procedimiento Facturación se divide en los siguientes pasos.

- **Paso 1:** El funcionario Administrativo de la Oficina de Partes recibe las facturas y las deriva al Encargado de Facturación de Abastecimiento.
- **Paso 2:** Los Jefes de Departamento reciben las Facturas. Verifica que se encuentren bien, de ser así las firma y las deriva al Encargado de Facturación de Abastecimiento, de encontrar errores en las facturas estas se devolverán a los proveedores.
- **Paso 3:** El Encargado de Recepción Física de Abastecimiento recibe los productos, si estos llegan con factura envía factura original a Encargado de la Unidad de Rendición de Facturas de abastecimiento, y la copia al Encargado de Recepción por Sistema Abastecimiento. De no llegar la factura se envía guía de despacho a recepción por sistema.

Los pasos 1, 2 y 3 pueden funcionar paralelamente siendo cualquiera de ellas quienes inicien el proceso.

- **Paso 4:** El Encargado de Facturación de Abastecimiento revisa y registra la documentación luego procede a registrar en planilla de control, archiva facturas en espera de recepciones.
- **Paso 5:** Encargado de Recepción por Sistema Abastecimiento entrega recepciones (productos recibidos), junto a Guía de Despacho o copia de Factura según corresponda.
- **Paso 6:** El Encargado de Facturación de Abastecimiento verifica la documentación, busca Factura y Orden de Compra asociadas a la recepción. El encargado decide si el proceso continúa, de encontrar algún inconveniente, decide que no prosiga y devuelve factura al proveedor o solicita ajustes a lo recepcionado según corresponda. Si decide que el proceso prosiga. Registra el estado de la factura y pasa a encargado de devengar por sistema en Contabilidad. El Encargado de Facturación de Abastecimiento elabora informe mensual de facturas en abastecimiento.
- **Paso 7:** El Encargado de la Unidad de Rendición de Facturas emite listado de facturas a rendir, adjunta Facturas y documentos soportantes y envía a Contabilidad.
- **Paso 8:** El Encargado de Control Interno de Contabilidad verifica la documentación. Si detectase algún error no autoriza que continúe el proceso, devolviendo los documentos. Si autoriza, registra el visto bueno a la factura y pasa a encargado de devengar por sistema en contabilidad.
- **Paso 9:** El Encargado de Ejecución Presupuestaria revisa la documentación, ingresa datos de la Factura con montos por ítem presupuestario y procesa para búsqueda de la recepción en el sistema (sustento) y procede a procesar devengamiento. Archiva Facturas en kardex de Facturas a cancelar.

2.4.4. Procedimiento de Programa Anual de Compras

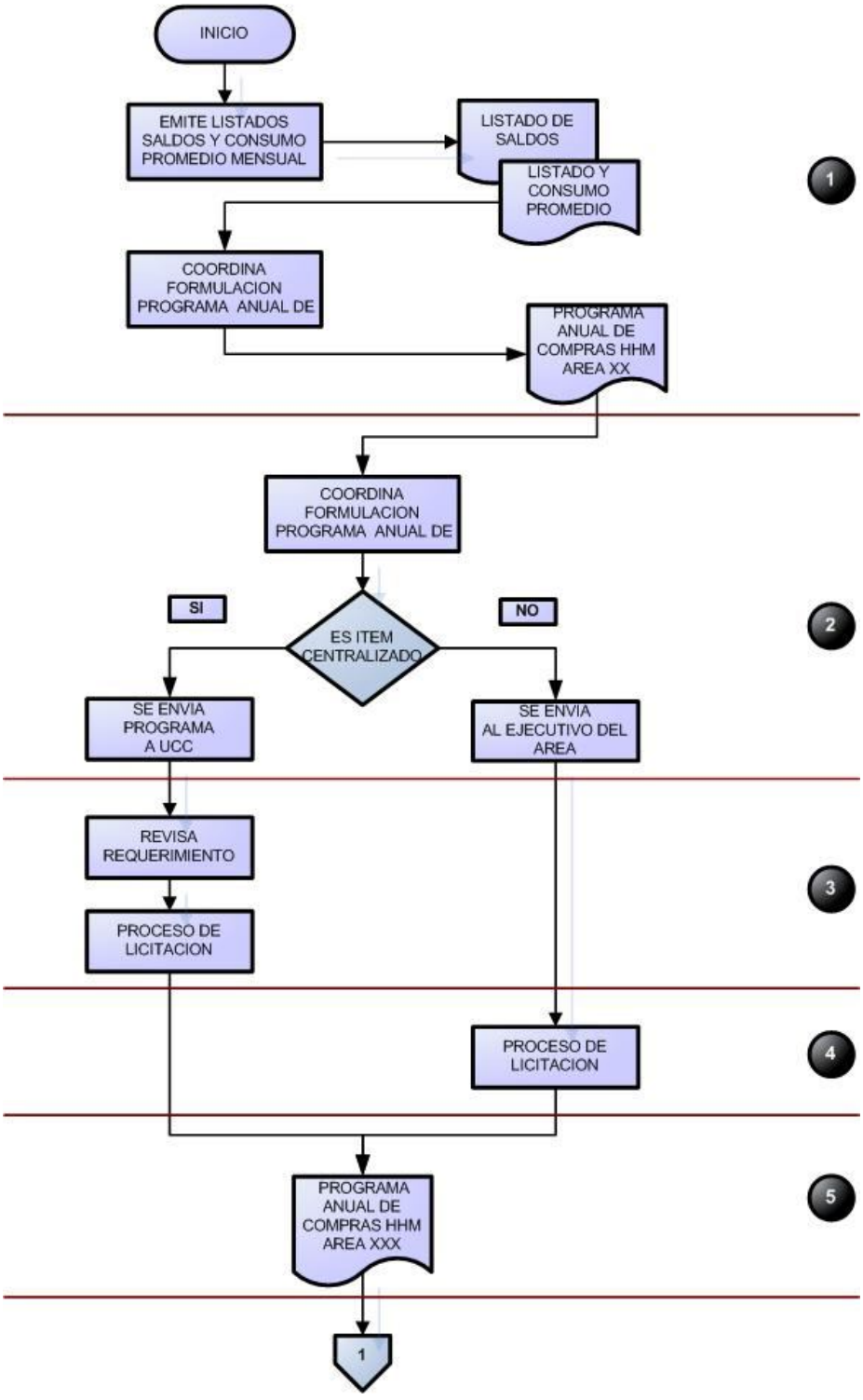

Figura 8: Procedimiento de Programa Anual de Compras Parte 1

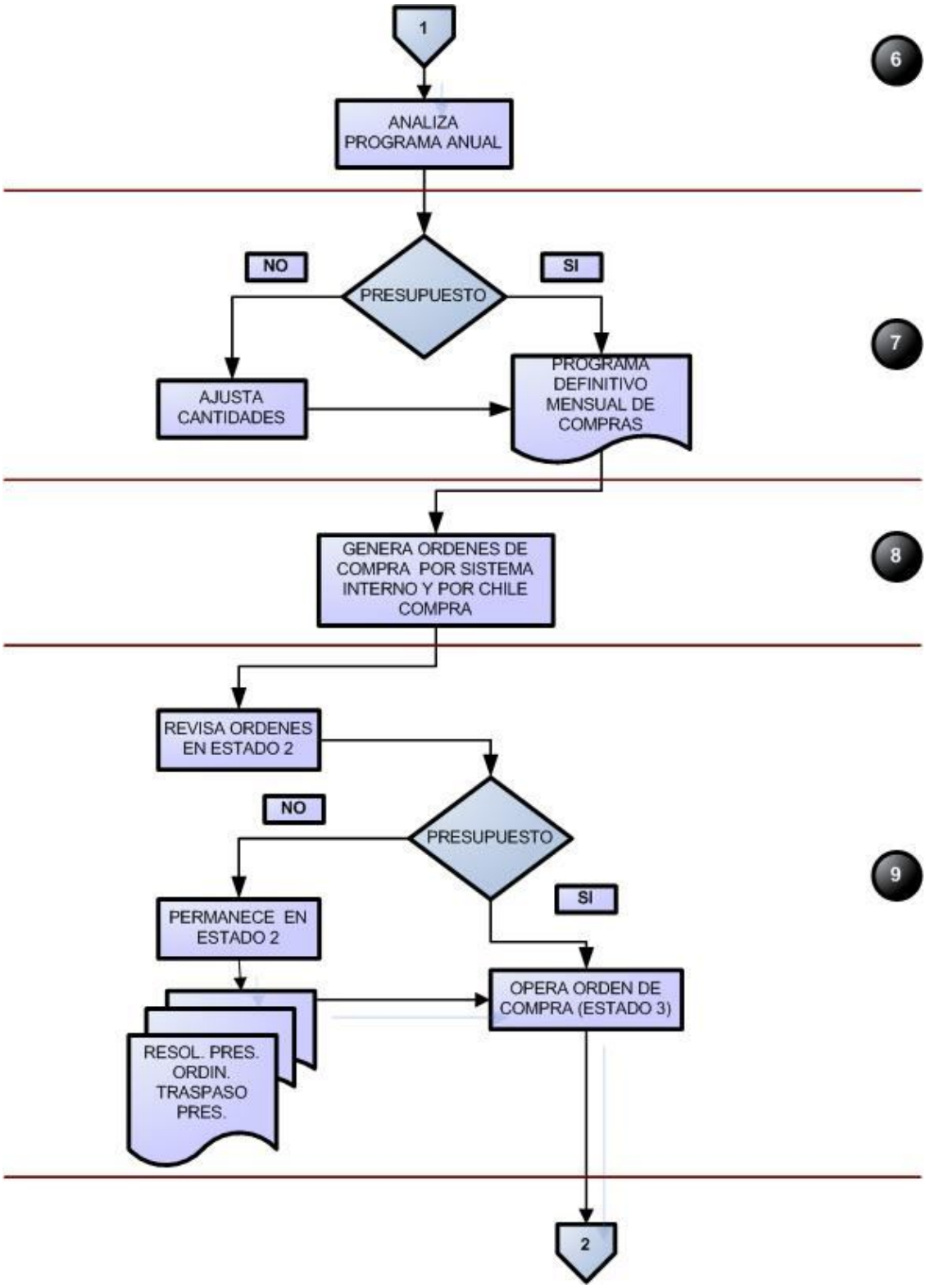

Figura 9: Procedimiento de Programa Anual de Compras Parte 2

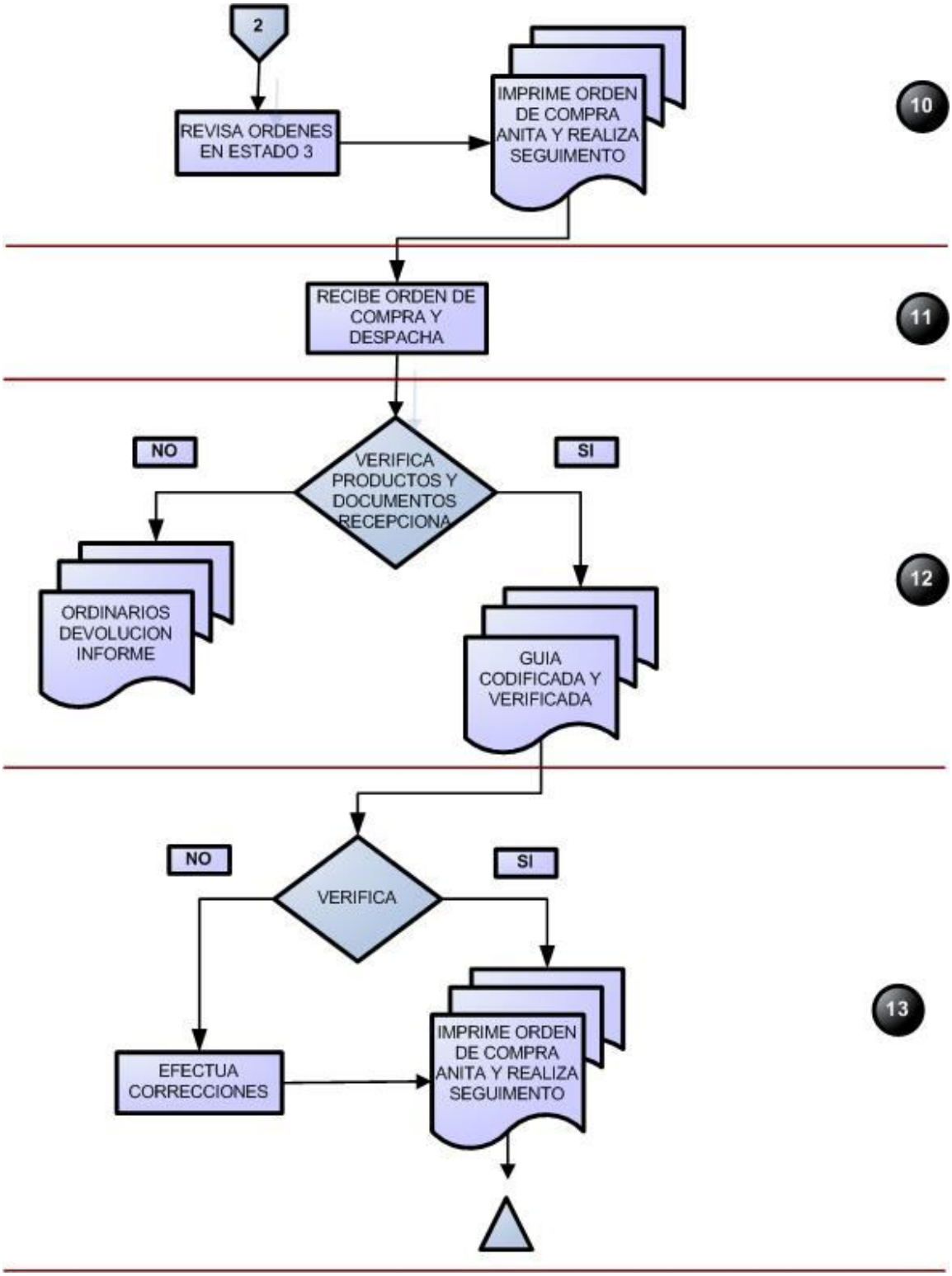

Figura 10: Procedimiento de Programa Anual de Compras Parte 3

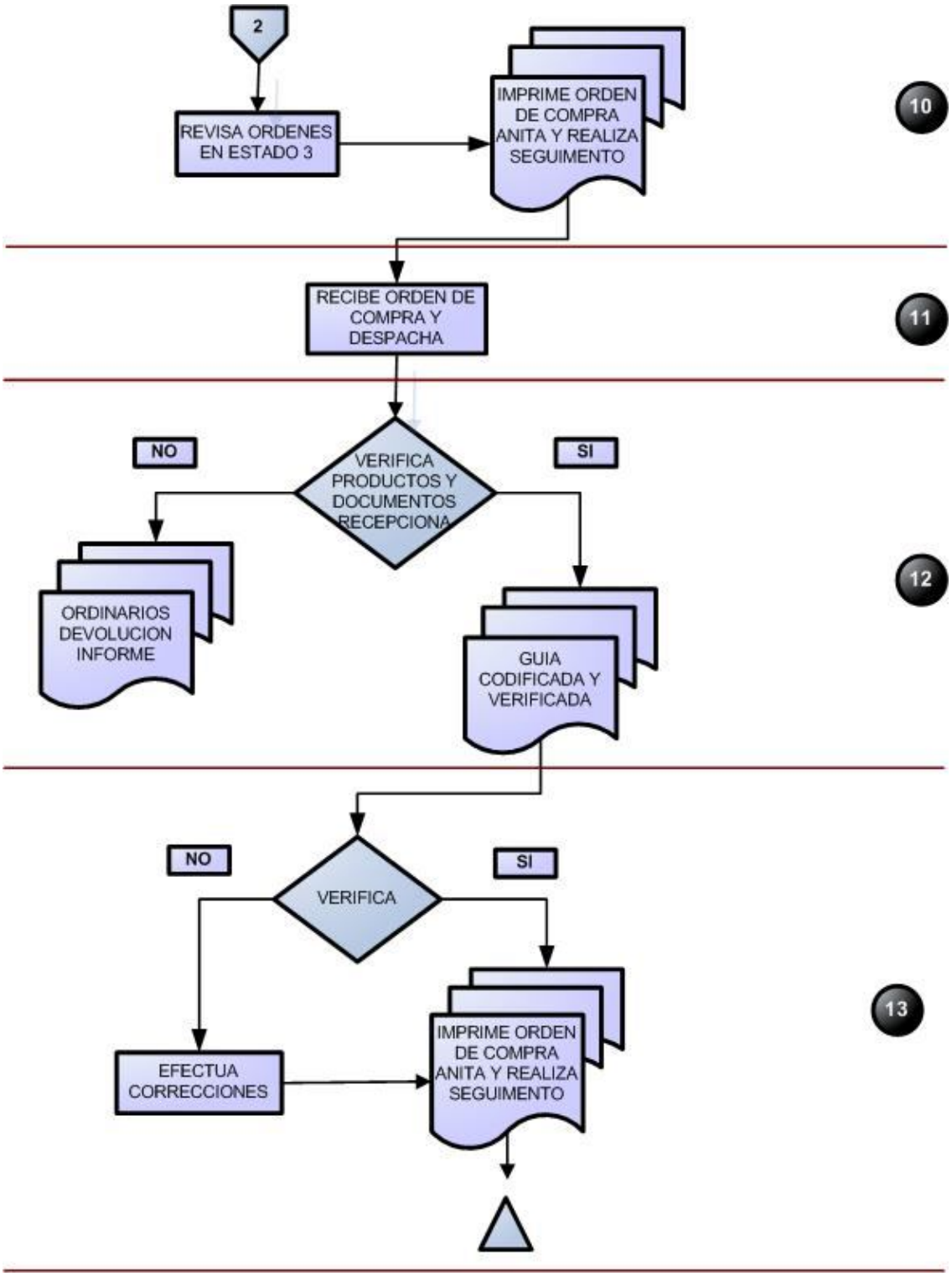

Figura 11: Procedimiento de Programa Anual de Compras Parte 4

Descripción Procedimiento de Programa Anual de Compras.

Este procedimiento tiene como finalidad la ejecución del programa anual de compras del HCHM, el cual se ejecuta mensualmente. El Personal que interviene en dicho procedimiento es el siguiente:

1. Ejecutivos de Compras.
2. Jefe de la Sección de Abastecimiento.
3. Jefe de Unidad de Compra del Servicio Salud Ñuble.
4. Proveedores.
5. Encargado de Recepción de Bodega.

El procedimiento de Programa Anual de Compras se divide en los siguientes pasos.

- **Paso 1:** Los Ejecutivos de Compras deben comprobar los saldos disponibles en bodegas, en el sistema y físicamente. Además determinar el consumo promedio mensual de cada producto. Un Ejecutivo de Compras coordina la emisión del programa de compras, efectuando reuniones de trabajo con las entidades involucradas, usuarios, Encargado de Recepción de Bodega, Jefe de la Sección de Abastecimiento, en las que se analizan consumos promedios, saldos, estacionalidad en el consumo de productos. Cumplido este paso de emite el programa anual de compras por área.
- **Paso 2:** El Jefe del Sección de Abastecimiento verifica el programa de compras anual y analiza si es ítem centralizado.

  Si es centralizado se envía a la unidad de compras del servicio de salud Ñuble para su verificación.

  Si no es centralizado se deriva a los ejecutivos de compras especializados de cada área para llevar a cabo la licitación.
- **Paso 3:** El Jefe de la Unidad de Compras del Servicio de Salud Ñuble recibe vía correo electrónico el programa anual de compras y verificando la información entregada. Posteriormente realiza la licitación.

La Unidad de Compras del Servicio de Salud Ñuble recepciona las cotizaciones, valoriza los requerimientos de acuerdo a la mejor opción económica, y emite programa anual de compras.

- **Paso 4:** el Jefe de la Sección Abastecimiento recibe el programa anual de compras valorizado, y consolidada con los distintos programas de compras de cada Ejecutivo de Área, efectuando el análisis y encuadre presupuestario. Remite a Finanzas para efecto de elaboración presupuestaria.
- **Paso 5:** El Ejecutivo de Compras del Sección de Abastecimiento analiza requerimiento mensual del programa de compras, para ello revisa el stock actual de las bodegas y realiza los ajustes a los pedidos que reflejen la realidad actual.
- **Paso 6:** El Jefe de la Sección Abastecimiento verifica que el pedido se encuadre en el marco presupuestario vigente de acuerdo a la resolución que autoriza presupuesto mensual por ítem del Sub-Título 22 (Bienes y Servicios de Consumo).

  Si este no se ajusta se procede a efectuar rebajes en las cantidades del pedido con el fin de mantenerse dentro del marco presupuestario.

  Si se ajusta se le da el visto bueno, cerrando el programa de compras definitivo del mes instruyendo al ejecutivo de compras del área continuar con el proceso de adquisiciones.
- **Paso 7:** El Ejecutivo de Compras del área genera ordenes de compra en Sistema ANITA y por Mercado Público. Envía la orden de compra a sección contabilidad en forma electrónica para su respaldo presupuestario (Obligación Presupuestaria). Al generar la propuesta y traspasarla al Departamento de Contabilidad ésta se encuentra en estado 2 para el sistema.
- **Paso 8:** El personal Encargado de la Unidad de Presupuesto del Departamento de Contabilidad, comprueba las órdenes en estado 2 (ver ANEXO VII), comprobando la disponibilidad presupuestaria según imputación.

  Si no hay disponibilidad presupuestaria la orden de compra se mantiene en estado 2 hasta que se recepcione una solicitud de traspaso presupuestario del responsable del ítem o una resolución del SDA (Subdirección Administrativa)

que autoriza el presupuesto extraordinario o sobregiro. Si hay disponibilidad presupuestaria se autoriza la orden pasando a estado 3.

- **Paso 9:** El Ejecutivo de Compras de Abastecimiento imprime la orden de compra en quintuplicado, tramita firmas y despacha a proveedores realizando distribución interna de ejemplares (Unidad de Facturación), responsable ítem presupuestario, archivo correlativo), ejecutando seguimiento de la orden.
- **Paso 10:** Los Proveedores reciben la Orden de Compra, preparan pedido y despachan artículos requeridos a Unidad de Almacenamiento y Distribución del Hospital.
- **Paso 11:** El Encargado de Recepción de Bodega recibe los artículos, compara con la orden de compra, verifica precio y cantidad comparando con Factura o guía del despacho, verifica estado de productos recepcionados.

  Si detecta algún error se procede a realizar la devolución, generando ordinarios de devolución, detallando el envío se incluye la Factura e informando al ejecutivo de Compras del área, la condición en la cual llegaron los artículos (cantidad y calidad).

  Si no se detecta error se procede a codificar y designar Auxiliar (funcionario encargado del procesamiento del pedido) para encasillar y entregar guía de despacho o copia de la Factura codificada a encargado de recepción de sistema, entregando la información necesaria para considerar ajuste que se generan por diferencias provocadas por procedimiento de compras del Hospital. Se envía Factura original a Encargado de Rendir Facturas.
- **Paso 12:** El encargado de recepción de sistema verifica la información recibida en la guía de despacho o factura contrarestada con la orden de compra poniendo énfasis en los valores de conversión, precio y cuadratura.

  Si se detectan errores se efectúan las correcciones correspondientes.

  Si no se detectan errores se emite documento de recepción en triplicado entregando copia a facturación.

2.4.5. Procedimiento para dar de Baja Fármacos y Productos Comunes

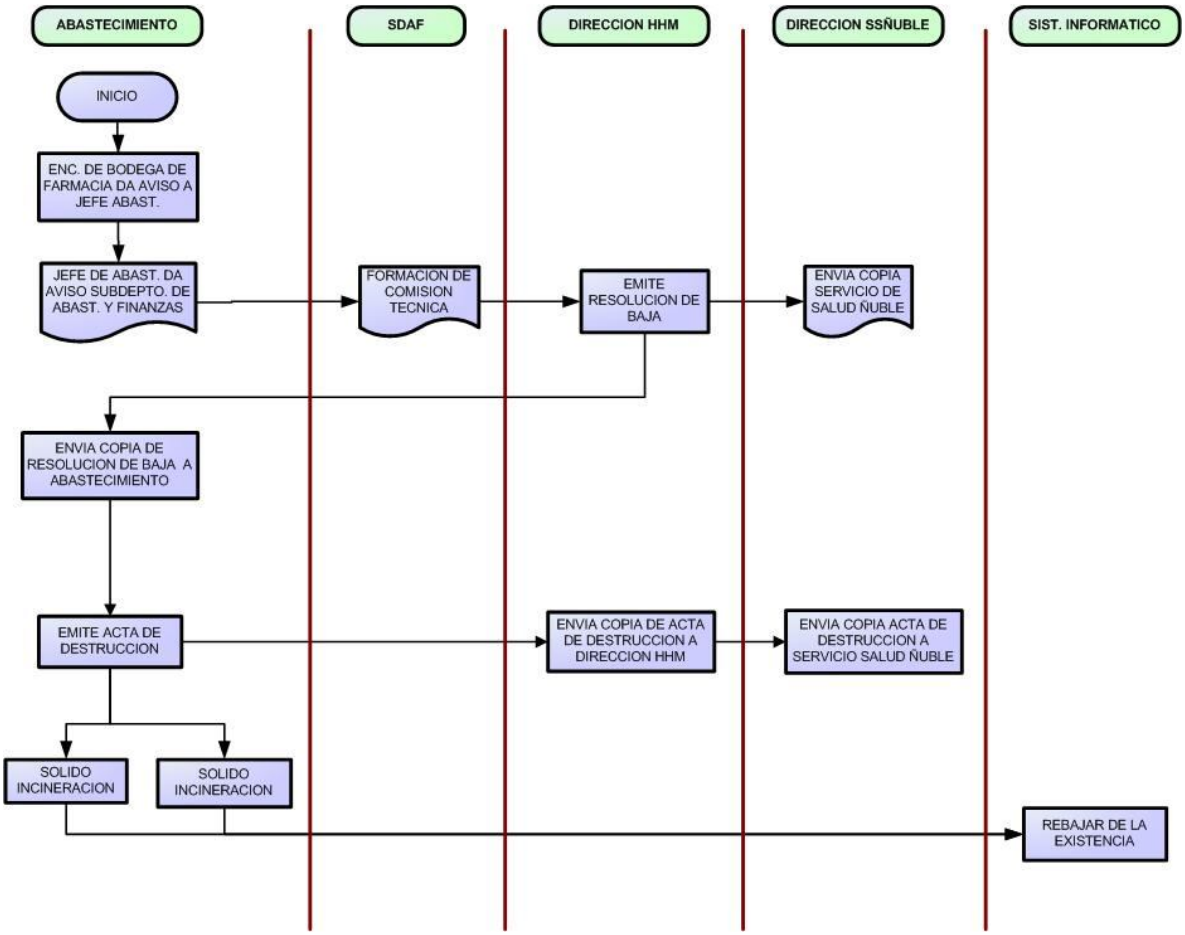

Figura 12: Procedimiento Para dar de Baja Fármacos y Productos Comunes

Descripción para dar de Baja Fármacos y Productos Comunes.

Este procedimiento es realizado con el fin de dar de baja los insumos, sean estos fármacos o productos generales, que por algún criterio no puedan mantenerse disponibles en bodega, o ser utilizados por alguna unidad. Estos deberán eliminados tanto física como lógicamente del sistema ANITA.

El procedimiento para Dar de Baja Fármacos y Productos Comunes se divide en los siguientes pasos.

- **Paso 1:** El proceso se inicia cuando el Encargado de Bodega de Farmacia comunica al Jefe de Abastecimiento el listado de insumos que deben ser dado de baja. El Jefe de Abastecimiento comunicará esta solicitud al Subdepartamento de Abastecimiento y Finanzas.
- **Paso 2:** El Subdepartamento de Abastecimiento y Finanzas procederá a llamar la formación de una comisión técnica que evalué el caso y si procede la eliminación.
- **Paso 3:** El Director del Hospital emite la resolución de baja del insumo.
- **Paso 4:** De forma simultánea se genera una copia de la resolución de baja al servicio de salud de Ñuble y la Sección de Abastecimiento.
- **Paso 5:** En la Sección de Abastecimiento, una vez recepcionada la resolución se procede a generar el acta de destrucción de los insumos. Se le envía una copia del acta generada a la Dirección del Hospital.
- **Paso 6:** La Dirección del Hospital envía copia del acta de destrucción al Servicio de Salud Ñuble.
- **Paso 7:** Se procederá a la destrucción de los insumos. En caso de que los productos a eliminar sean sólidos, estos se destruyen por incineración en dependencias del Hospital. En caso de ser líquido se procede a su eliminación por drenaje.
- **Paso 8:** Se da aviso al sistema informático para rebajar la existencia de las bodegas. Dejando como registro el número de la resolución que lo dio de baja.

2.5. Área de Soporte de Comunicaciones

2.5.1. Objetivo

Velar por el buen funcionamiento de la red de comunicaciones, servidores y equipamiento computacional del Servicio de Salud Ñuble y de los establecimientos dependientes y asesorar a los usuarios en la resolución de problemas cotidianos computacionales.

2.5.2. Dependencia Jerárquica

a) Depende de: Departamento Recursos Físicos

b) Secciones dependientes: No tiene

2.5.3. Dependencia Funcional

No tiene

2.5.4. Relaciones de Asesoría

a) **Presta asesoría a**:

Todos los usuarios del Servicio de Salud Ñuble y de todos los establecimientos dependientes que necesiten una asesoría computacional.

b) **Recibe asesoría de:**

- Servicio Técnico externo.
- Subdepto. Tecnologías de la Información de la Dirección de Servicio.
- Oficina de Ingeniería de Sistemas HCHM.

2.5.5. Relaciones Funcionales

a) **Internas:**

Se relaciona funcionalmente con todas las secciones y unidades existentes en cada establecimiento del Servicio de Salud Ñuble.

b) **Externas:**

- Servicio Técnico Externo.
- Empresa Telefónica por Proyecto Red del Ministerio de Salud (MINSAL).
- GRIFOLS Chile S.A. por Proyecto Dispensadores de Farmacia HCHM.

2.5.6. Funciones Generales

1. Soporte Usuarios de todos los establecimientos dependientes del Servicio de Salud Ñuble.
2. Mantención operativa de la red de comunicaciones de voz y datos.
3. Resolución de Problemas computacionales de los usuarios de toda la red del Servicio de Salud Ñuble.

4. Monitoreo y administración de recursos de la red.
5. Respaldo de la información de servidores principales.
6. Mantención de los inventarios computacionales.
7. Mantención operativa de la Red de Videoconferencia

2.6. Descripción de los Sistemas de Información

2.6.1. Sistema ANITA – Módulo ABASUR

El Sistema de Abastecimiento está estructurado en 8 módulos que funcionan independientemente, pero que comparten información entre sí, estos son: Funciones Básicas, Proveedores, Cotizaciones, Compras, Bodega, Programación de Compras, Unidad de Producción e Inventario. La finalidad de éstos es entregar los mecanismos por medio de los cuales se pueda manejar y monitorear constantemente la evolución de las Cotizaciones y Compras que son manejadas por los Servicios de Salud, como también los procesos de Recepción y Distribución de los productos que están directamente relacionados con Bodega.

Se han establecido una serie de Estándares para el manejo de las pantallas y procesos, como una manera de agilizar la ejecución de éstos y hacerla más cómoda al usuario, estos estándares generales se describen a continuación.

2.6.2. Menú Principal del Sistema ANITA

La Figura 13 muestra el menú principal del módulo de abastecimiento una vez el usuario se autentificad. Se despliegan las distintas opciones de operación que se pueden realizar.

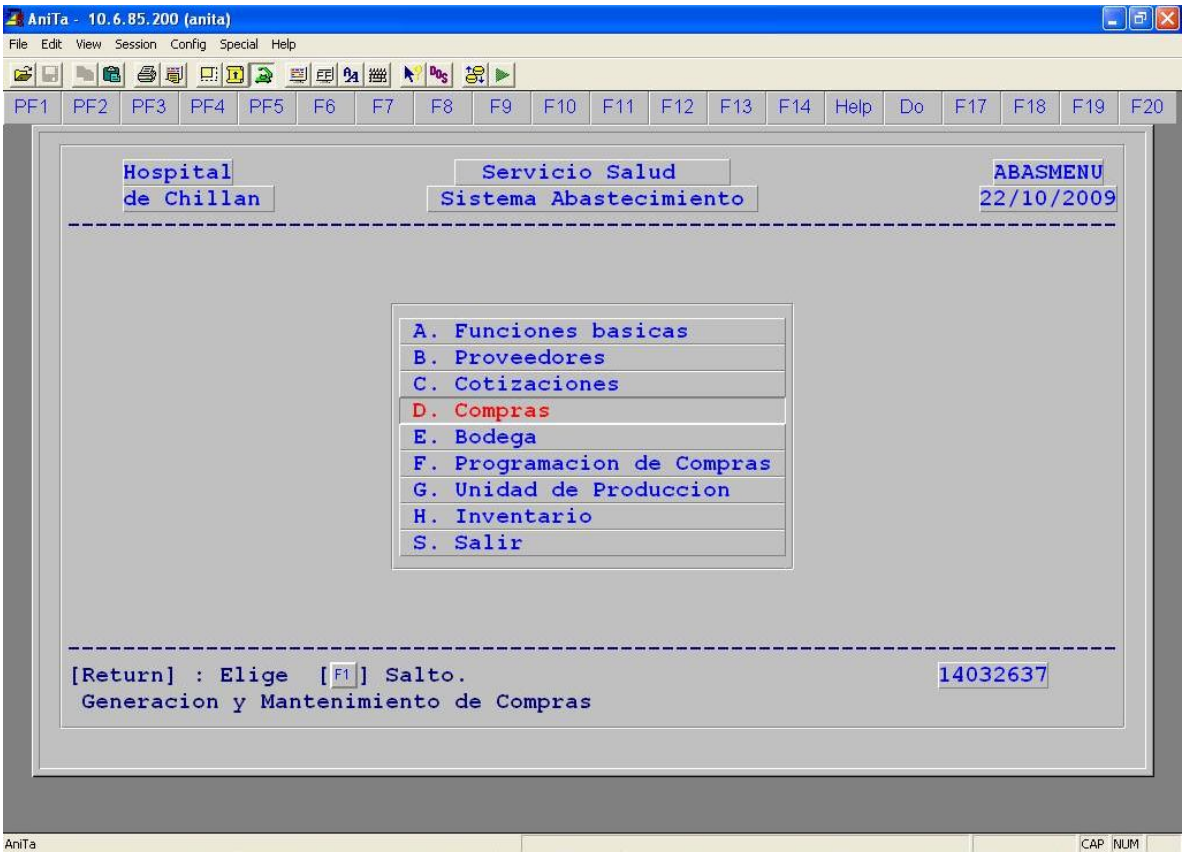

Figura 13: Menú Principal Módulo ABASUR

2.6.3. Menús de Procesos

Los procesos o módulos ejecutables, presentan también menús a través de los cuales el usuario podrá ejecutar ciertas operaciones, o bien seleccionar una opción del menú que le permita efectuar ciertas operaciones dentro del proceso.

Estos menús se presentan de la siguiente manera.

```
+-------------------------------------------------------------------------+
|  IBM                        FUNCIONES BÁSICAS                  abfbt001  |
|de Chile                  Manutención de Productos                       |
|MENÚ:   Ingresa  Modifica  Elimina  Consulta  Ver  Reporte  Termina      |
|Ingresar una nuevo Registro                                              |
|-------------------------------------------------------------------------|
```

Figura 14: Menú de Procesos

2.6.4. Funciones del Menú Principal

2.6.4.1. Funciones Básicas

El módulo de Funciones Básicas es aquel a través del cual son mantenidas un conjunto de tablas necesarias para el correcto funcionamiento del sistema. Las únicas operaciones que se realizarán aquí serán las de ingreso, modificación o eliminación de los datos que éstas contengan.

Dentro del conjunto de tablas que son mantenidas, existen dos grupos particulares, las de Tipos y Estados, las cuales no pueden ser modificadas, dado que los datos que éstas contienen son indispensables para el funcionamiento del sistema. Estas tablas sólo presentan la opción de consulta.

Las demás tablas pueden ser modificadas cuando se estime conveniente.

Descripción

En este módulo es posible mantener todas las tablas básicas como lo son los productos, rubros, subrubros, rubros básicos, relación de rubros, unidades, imputaciones, estados, tipos, etc.

Dentro del módulo de funciones básicas se encuentra el siguiente menú de navegación:

A. Productos
B. Rubros
C. Sub Rubros
D. Rubros Básicos
E. Relación de Rubros
F. Unidades
G. Usos
H. Producto - Marca Proveedor
I. Consulta Producto v/s Producto Marca Proveedor
J. Otros Mantenedores
K. Mantenedores Tablas de Estado y Tipo

A. Productos

Todos los módulos del Sistema trabajan en base a la lista de productos que existan en el maestro de productos, los cuales deberán ser ingresados a través de este proceso, el que a su vez permite modificar o eliminar productos según las necesidades. Cada uno de los productos creados son identificados a través de un código.

Para poder ingresar productos es necesario que hayan sido actualizadas previamente las tablas de **Rubros**, **Sub Rubros, Rubros Básicos, Relación de Rubros, Unidades y Usos** dado que son datos que el mantenedor solicitará.

Las operaciones que pueden ser llevadas son; Ingresa, Modifica, Elimina, Consulta, Ver, Reporte, Termina.

B. Rubros, SubRubros, Rubro Básico, Relación de Rubros, Unidades y Usos

Las 6 tablas mencionadas deben estar ingresadas antes de poblar la tabla de productos, ya que en aquel procedimiento se requiere hacer referencia a estas tablas como datos obligatorios.

La tabla rubros contiene un código que hace referencia a una categoría de productos, la cual es única y debe ser descrita.

H. Producto – Marca Proveedor

En este mantenedor se crearán todos los productos específicos asociados a los proveedores.

Las operaciones que se pueden realizar son; Ingresa, Modifica, Elimina, Reporte, Consulta y Ver.

I. Consulta Producto v/s Producto Marca Proveedor

Esta función permite consultar por los subproductos asociados a un producto y su correspondiente codificación Central Nacional de Abastecimiento (CENABAST) si corresponde. Pudiendo seleccionar los productos que se desee de acuerdo a criterios que se desee.

J. Otros Mantenedores

La Opción Otros Mantenedores mantiene las tablas de Calificación de Proveedores, Centros de Costo, Formas de Pago, Ubicación Física de Bienes, Bodegas, Observación Salida Bodegas, Mantenedor de IVA, Mantenedor de tipo de Documento Contable y Mantenedor Folios de Documentos, todas necesarias para el funcionamiento integrado de los módulos que conforman el sistema.

K. Mantenedores de Tablas de Estado y Tipo

Las únicas operaciones disponibles en esta operación son las de Consulta y Reporte, siendo sus valores dados por el sistema y de carácter inmodificable.

2.6.4.2. Proveedores

El módulo de Proveedores permite llevar a cabo la mantención del registro de Proveedores que manejará el Servicio de Salud, así como los convenios que se establezcan entre los servicios y éstos.

El menú de Proveedores se divide en tres opciones, el mantenedor de Proveedores propiamente tal, el mantenedor de Convenios y una Consulta de Proveedores por rubro. El mantenedor de Proveedores permite llevar a cabo todas las operaciones necesarias sobre ellos, y el mantenedor de Convenios permite establecer y manejar estos últimos.

Descripción

Este módulo permite las siguientes operaciones; Ingresa, Actualizan, Elimina, Consulta y obtener reportes los proveedores y los convenios.

Dentro del módulo de Proveedores se encuentra el siguiente menú de navegación:

A- Registro de proveedores

B- Convenios

C- Consulta de Proveedores por Rubro

D- Consulta de Compras por Convenio

E- Comportamiento de Proveedores por Periodo

A. Registro de Proveedores.

El mantenedor de Proveedores permite ingresar, modificar, eliminar, consultar y calificar a todos los Proveedores mantenidos en el sistema.

Para el ingreso de los nuevos proveedores se deben ingresar datos como;

- Rut de del proveedor.
- Tipo, esto es si es natural o jurídico, de ser natural se capturan datos como nombre, apellido.
- Código, que permite identificar al proveedor de manera única independiente de su rut.
- Razón Social, solo si es de tipo jurídico.
- Estado, si el proveedor se encuentra habilitado o no.
- Rubro, se indica el rubro al cual pertenece el proveedor.

Esta opción cuenta además con funcionalidades como modificar, eliminar, consultar el registro maestro, ver detalle, contactos y reportes.

B. Convenios

Este módulo permite mantener los convenios establecidos entre un Proveedor y el Servicio de Salud con respecto a la compra de ciertos productos que el proveedor ofrece.

La pantalla principal del mantenedor es la siguiente:

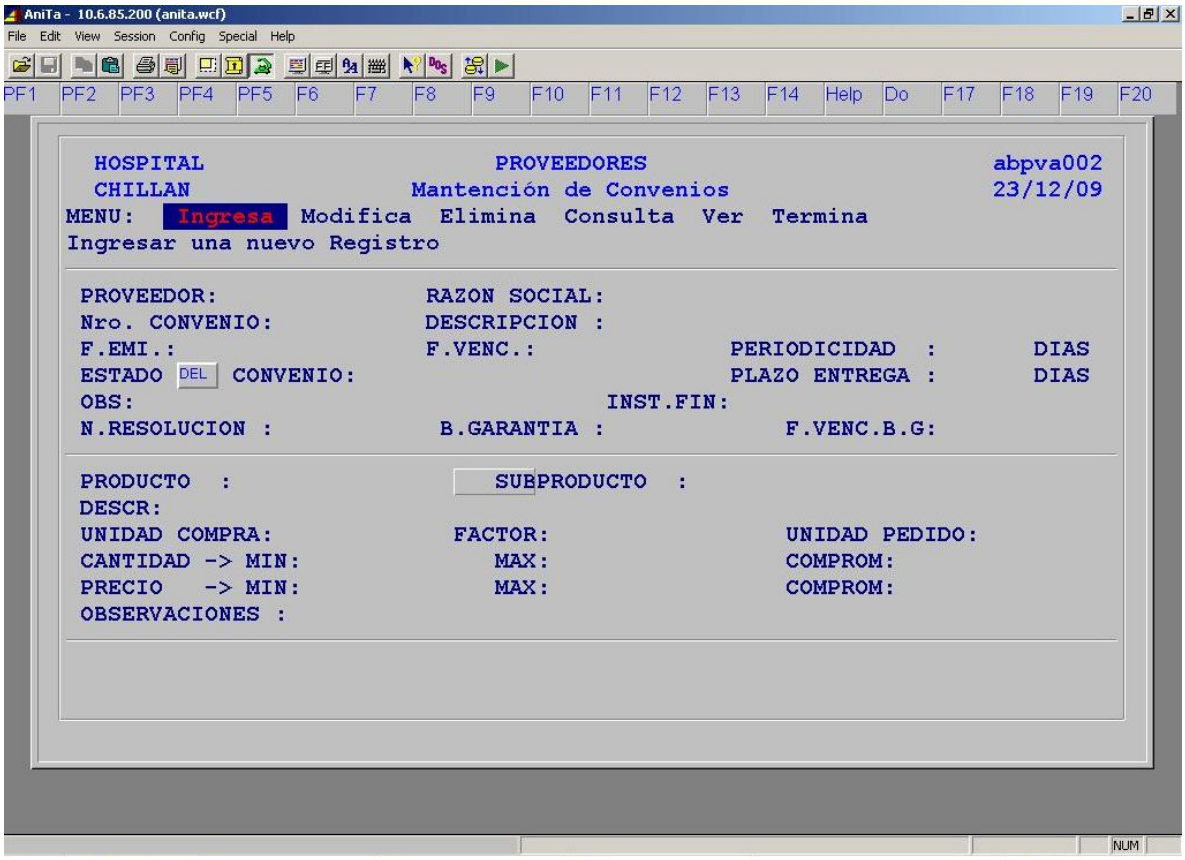

Figura 15: Menú Mantención de Convenios

Para el Ingreso de nuevos convenios se requieren algunos datos como;

- **Proveedor,** se ingresa el Rut del Proveedor, o se selecciona uno de la Tabla de Proveedores. Una vez ingresado éste, se desplegará la **Razón Social** del mismo.
- **Nro. Convenio,** este campo se genera automáticamente por el sistema al grabar el convenio.
- **Descripción,** se ingresa una descripción del convenio que se va a crear.
- **F. Emi.** Se ingresa la fecha en que es emitido el convenio.
- **F. Venc.** Se ingresa la fecha de vencimiento del convenio.
- **Periodicidad**, se ingresa en días la frecuencia de compras que existirá bajo este convenio.
- **Estado Convenios, s**e ingresa el estado del convenio el cual puede ser activo o inactivo.
- **Plazo de Entrega, s**e ingresa en días el plazo de entrega que tienen los productos del convenio.

Una vez que se ingresan los datos del convenio se deben registrar los productos del convenio, algunos datos de este registro son los siguientes:

- **Producto, s**e ingresa el código del producto.
- **Subproducto**, se ingresa el subproducto asociado al producto ingresado anteriormente.
- **Unidad,** se indica la unidad en que se manejará el producto del convenio, Ejemplo de ello son kilogramos, miligramos etc.
- **Factor,** se ingresa el factor de conversión de la unidad. Factor que transforma la unidad de compra en unidad de pedido.
- **Cantidad mínima,** se ingresa la cantidad mínima que se puede comprar a través del convenio.
- **Cantidad máxima,** se ingresa la cantidad máxima que se puede comprar a través del convenio.
- **Cantidad comprometida,** es la cantidad que se comprará a través del convenio habitualmente.
- **Precio mínimo,** Es el precio mínimo que se le asigna al producto asociado a la cantidad mínima.
- **Precio máximo,** Es el precio máximo que se le asigna al producto asociado a la cantidad máxima.
- **Precio comprometido,** Es el precio que se pacta y está asociado a la cantidad comprometida.

El ingreso de producto se realiza tantas veces como productos se comprometan en cada convenio.

El módulo convenios tiene otras funcionalidades como modifica, elimina, consulta, ver y termina.

C. Consulta de Proveedores por Rubro.

Esta opción permite ver todos los proveedores que pertenecen a un rubro. Para ello se deberá realizar la consulta con el rubro a buscar.

D. Consulta Compras por Convenio

Permite consultar bajo un convenio específico todos los productos comprados o en trámite de compra efectuados para ese convenio. Para ello se debe ingresar en la consulta el número del convenio.

E. Comportamiento de Proveedores por Periodo

Permite consultar para un periodo determinado la calificación dada a los diferentes proveedores que se relacionan con el Servicio de Salud.

2.6.4.3. Cotizaciones

El módulo de cotizaciones permite generar solicitudes de cotización de los Centros de Costo, solicitudes de cotización a proveedores, ingresar las ofertas enviadas por los proveedores a través de cartas de cotización y/o lista de precios y finalmente provee de una consulta de precios que permite revisar los precios vigentes para uno o todos los productos.

Descripción

Módulo que permite mantener todo lo relacionado con cotizaciones, tales como, solicitudes de cotización, ingreso de cotizaciones y cartas a proveedores.

Dentro del módulo de Cotizaciones se encuentra el siguiente menú de navegación:

A- Solicitudes de Cotizaciones
B- Cotizaciones a Proveedores
C- Ingreso de Cotizaciones
D- Consulta Estado Cotizaciones
E- Consulta de Precios
F- Terminar.

A. Solicitudes de Cotización

Las solicitudes de Cotización son creadas en este módulo por los distintos centros de costos, en él se indican los productos a cotizar, así como la cantidad requerida. Luego estas solicitudes deben ser revisadas y así entran al proceso de generación de la carta de cotización al proveedor.

La función principal de este proceso es brindar a los Centros de Costos un medio para solicitar a abastecimiento que les cotice uno o varios productos a distintos proveedores.

La pantalla principal es la siguiente:

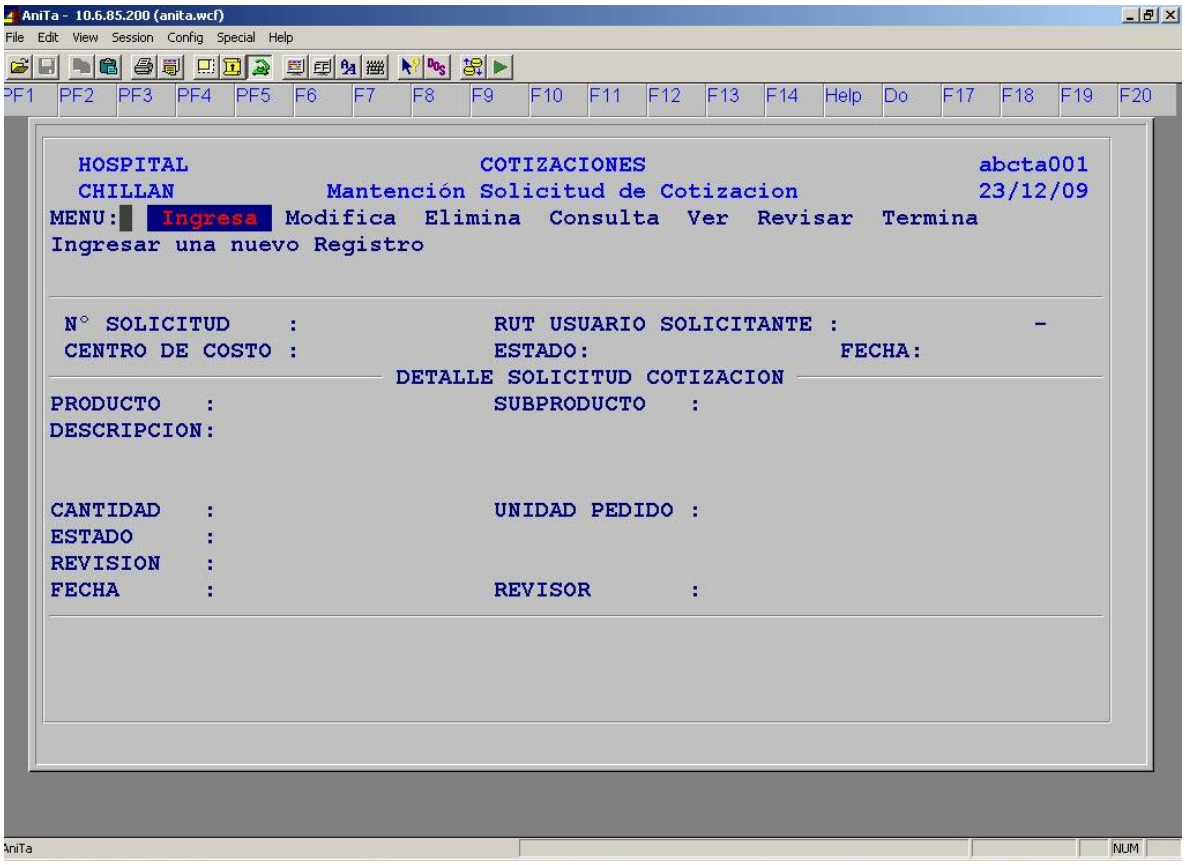

Figura 16: Menú Mantención Solicitud de Cotización

El Ingreso de Solicitudes de los diferentes centros de costos, debe contener los siguientes datos:

- **Producto,** se ingresa el código del producto a cotizar.
- **Subproducto,** se debe ingresar el subproducto asociado al producto que se desea cotizar (detalle del producto).
- **Cantidad.** Se ingresa la cantidad deseada del producto.
- **Unidad Pedido.** Se asigna automáticamente la unidad de pedido del producto (No modificable).

Las demás opciones de este módulo son modificar, eliminar, consultar, ver, revisar, reporte.

B. Cotizaciones a Proveedores

El proceso de Cotizaciones a Proveedores es el mecanismo a través del cual son generados e impresos los formularios de cotización a enviar a los proveedores. En él, para cada solicitud, se presenta en pantalla una lista de Proveedores a los que puede enviar el formulario.

También permite crear solicitudes de cotización directamente evitando pasar por la etapa de Solicitudes, y enviarla inmediatamente a los proveedores que correspondan; esto último será de utilidad para el administrador de abastecimiento en caso de que éste lo requiera; los Centros de Costo no tendrán acceso a este módulo.

C. Ingreso de Cotizaciones

A través de este proceso se ingresan las cotizaciones enviadas por los proveedores a los Servicios de Salud.

Las cotizaciones harán referencia a la solicitud que las originó, ingresándose los datos que correspondan a partir de la solicitud.

El ingreso de cotizaciones puede ser de 4 tipos, A, B, C o D. Las cotizaciones del tipo A son aquellas que hacen referencia a una solicitud de cotización enviada a los proveedores en el proceso anterior, las de tipo B corresponden al ingreso de Listas de Precios que los proveedores pudiesen enviar periódicamente, las de tipo C corresponden a Listas de Precios especiales por evento para casos como propuestas y las del tipo D corresponden a Listas de Precios por convenio.

Este proceso además cuenta con funcionalidades como, modificar, eliminar, consulta y ver.

D. Consulta Estado de Cotizaciones

Permite realizar consultas sobre el estado de las cotizaciones dentro de un periodo determinado para un Centro de Costo específico.

E. Consulta de Precios

La consulta de precios permite ver, dado un producto o un criterio de selección sobre el producto, todos los proveedores que lo ofrecen y cuyos precios estén vigentes

2.6.4.4. Compras

El módulo de compras es aquel por medio del cual se maneja toda la información relacionada con la compra de productos, tanto desde los Centros de Costo, como las efectuadas directamente por la Sección de Abastecimiento.

Descripción

Los procesos principales involucrados son la generación de Solicitudes de Compra por parte de los Centros de Costo, la revisión posterior de estas solicitudes, la Generación de Ordenes de Compras Consolidadas o individuales, y el envío de éstas a los Proveedores. El módulo tiene implementado consultas para poder seguir el desarrollo y vida de los procesos mencionados.

Cada una de las órdenes de compras generadas debe ser ingresada al portal Mercado Público, entrando en un proceso de licitación pública.

Dentro del módulo de Compras se encuentra el siguiente menú de navegación:

A- Administrar Solicitudes de Compra

- A.1- Solicitud de Compra por Cuadro Comparativo por Nómina de Producto.
- A.2- Mantención de Solicitud Compra por Nómina de Productos.
- A.3- Consultar Estados de Solicitudes de Compra
- A.4- Consulta de Cuadros Comparativos

B- Administración Órdenes de Compra

- B.1- Orden de Compra por Solicitud de Compra
    - B.1.1- Autorización Solicitudes de Compra
    - B.1.2- Generación de Orden de Compra por Solicitud
- B.2- Orden de Compra por Cuadro Comparativo por nomina de Productos.
- B.3- Mantención de orden de compra por nomina de Producto
- B.4- Orden de Compra Directa
- B.5- Consulta de Cuadros Comparativos
- B.6- Consulta Estado de Órdenes de Compra (OC)

C- Ajuste y Anulación de OC

- C.1- Ajuste por Exceso
- C.2- Ajuste por Déficit
- C.3- Anulación
- C.4- Consulta Ajuste Orden de Compra por Periodo

D- Histórico de Compras

- D.1- Ordenes por periodo y estado
- D.2- Ordenes por periodo y proveedor
- D.3- Ordenes por periodo y producto
- D.4- Ordenes por periodo y proyecto
- D.5- Ordenes por periodo y convenio
- D.6- Ordenes por periodo e imputaciones
- D.7- Ordenes por periodo
- D.8- Estratificación de Compras

E- Clasificación ABC

- E.1- Mantenedor Rangos
- E.2- Clasificación Automática ABC
- E.3- Consulta de Producto por Clasificación ABC
- E.4- Consulta de Productos por Clasificación VEN

F- Cierre de Año

- F.1- Ejecuta Cierre de Año
- F.2- Consulta Documentos Procesados por Cierre

Generalidades del Módulo de Compras

El Módulo de Compras se divide en dos grupos, el de Centros de Costo, y el de Abastecimiento. El grupo de Centros de Costo permite elaborar a éstos las solicitudes de compra de productos, así como seguir el estado de sus solicitudes hasta ser enviadas al

proveedor. El grupo de Abastecimiento analiza las solicitudes de los Centros de Costo, crea sus propias Ordenes de Compras, consolida las solicitudes de los centros de costo y las generadas por él, modifica, confirma y actualiza las solicitudes, y por último las envía a los proveedores correspondientes. Por supuesto también provee los procesos de selección de proveedores a los cuales se les comprarán los productos a través de los cuadros comparativos.

A. Administración de Solicitudes de Compra

Este proceso administra las Solicitudes de Compra, tanto para ingresar, modificar y eliminar las mismas

A.1. Solicitud de Compra por Cuadro Comparativo por Nomina de Producto.

Esta opción permite generar una solicitud de compra a partir de cuadros comparativos de acuerdo a una nómina de productos. Esta funcionalidad permite en un mismo procedimiento generar la nómina, los cuadros comparativos para los productos y las Solicitudes de Compra a cada proveedor.

A.2. Mantención de Sol. Compra por Nomina de Productos.

Esta función permite a los usuarios de los distintos Centros de Costo Modificar y Consultar las solicitudes de compra enviadas a Abastecimiento.

A.3. Consultar Estados de Solicitudes de Compra

Esta función permite consultar por el estado de las Solicitudes de Compra de los distintos Centros de Costo.

A.4. Consulta de Cuadros Comparativos

Esta función permite consultar por los cuadros comparativos del sistema utilizando diferentes criterios de selección.

B. Administración de Ordenes de Compras

Este proceso administra las Órdenes de Compra, ya sean por Convenios, Directas, Solicitud de Compra o por Nómina.

B.1. Órdenes de Compra por Solicitud de Compra

Esta opción genera las Órdenes de Compra a partir de Solicitudes de Compra emitidas por los diferentes Centros de Costo. Se presentan dos opciones:

- Autorización de Solicitudes de Compra, Esta función permite al Jefe de Abastecimiento autorizar las cantidades que los Centros de Costo solicitaron en su solicitud de compra. Sólo es posible autorizar las ordenes es estado Generadas.
- Generación de Órdenes de Compra por Solicitud, esta función permite generar la Orden de Compra.

B.2. Órdenes de Compra por Cuadro Comparativo por Nómina de Productos.

Esta función permite generar una Orden de Compra a partir de cuadros comparativos de acuerdo a una Nómina de Productos. Esta funcionalidad permite en un mismo procedimiento generar la nómina, los Cuadros Comparativos para los productos y generar la Orden de Compra.

Por otra parte permite generar Órdenes de Compra para las nóminas mensuales por rubro, es decir, permite generar Órdenes de Compra por Rubro a partir de aquellos productos solicitados a través del programa de compras por cada uno de los centro de costo.

B.4. Órdenes de Compra Directa

Este Proceso permite realizar Ordenes de Compra Directas, es estas son órdenes que no son sustentadas por Cuadros Comparativos, el usuario define el proveedor y el precio libremente.

La pantalla es la siguiente:

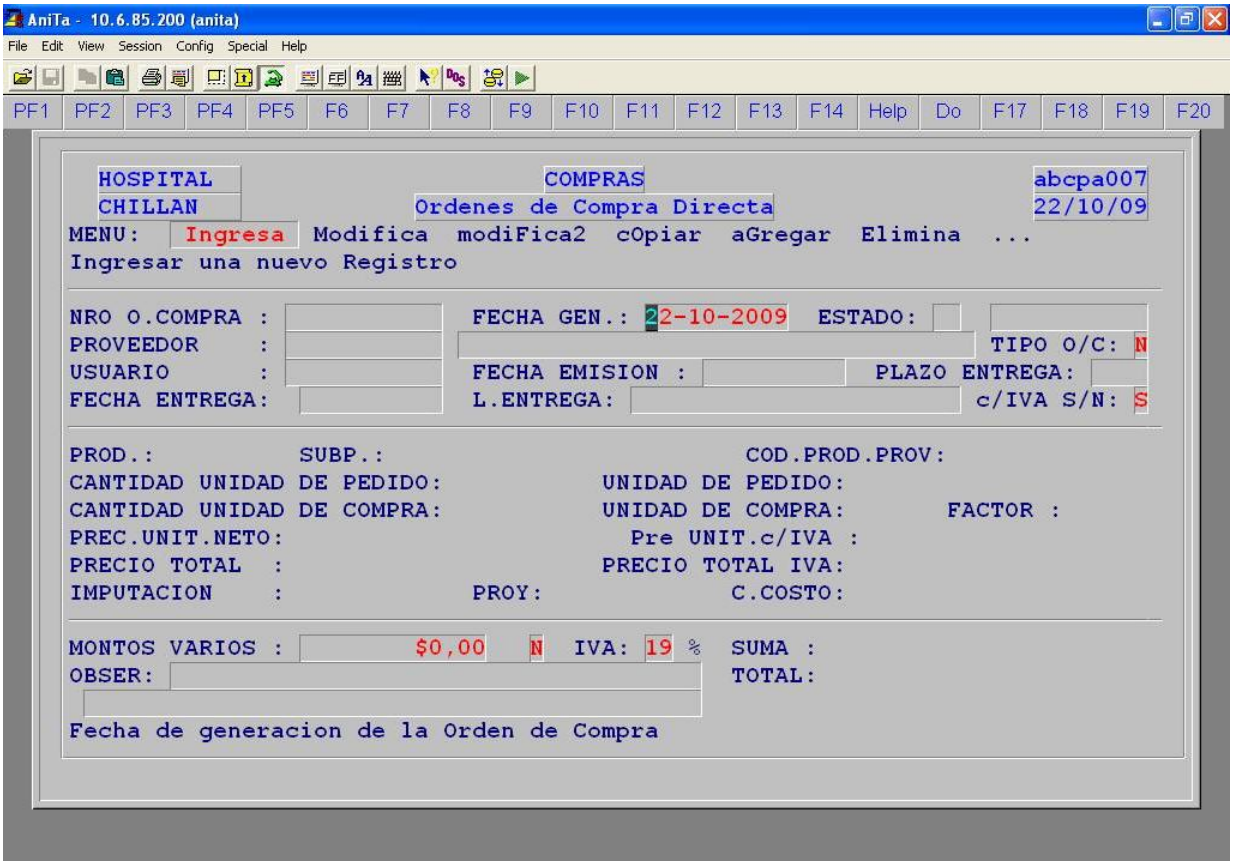

Figura 17: Menú Órdenes de Compra Directa

La opción de ingresar permite generar una orden de compra. Se deben ingresar los siguientes datos:

- Proveedor.
- Tipo de orden de compra, este puede ser normal, de consumo inmediato o un servicio.
- Plazo Entrega.
- Fecha Entrega.
- Lugar Entrega
- y si la orden de compra va con IVA o no.

Posterior a este proceso se ingresará el detalle de la Orden de Compra indicando los productos a solicitar.

B.5. Consulta de cuadros comparativos

Esta función permite consultar por los cuadros comparativos registrados en el sistema, utilizando diferentes criterios de selección.

B.6. Estados de Órdenes de Compra

Esta consulta permite ver en que estado están las Órdenes de Compra de un centro de costo para un periodo determinado.

C. Ajuste/Anulación Ordenes de Compra

Este Menú ofrece 3 opciones para dar la posibilidad de Anular Orden de Compra y Ajustarlas por Exceso o por Déficit. Los ajustes son por cantidades y no por precios.

C.1. Ajuste por Superávit

Esta función permite ajustar una Orden de Compra, si alguno de sus productos llega en exceso (más de lo solicitado). Para realizar el ajuste se crea una Orden de Compra idéntica a la que se quiere ajustar, pero con la cantidad de exceso. La cantidad en exceso se agrega al stock disponible.

La pantalla es la siguiente:

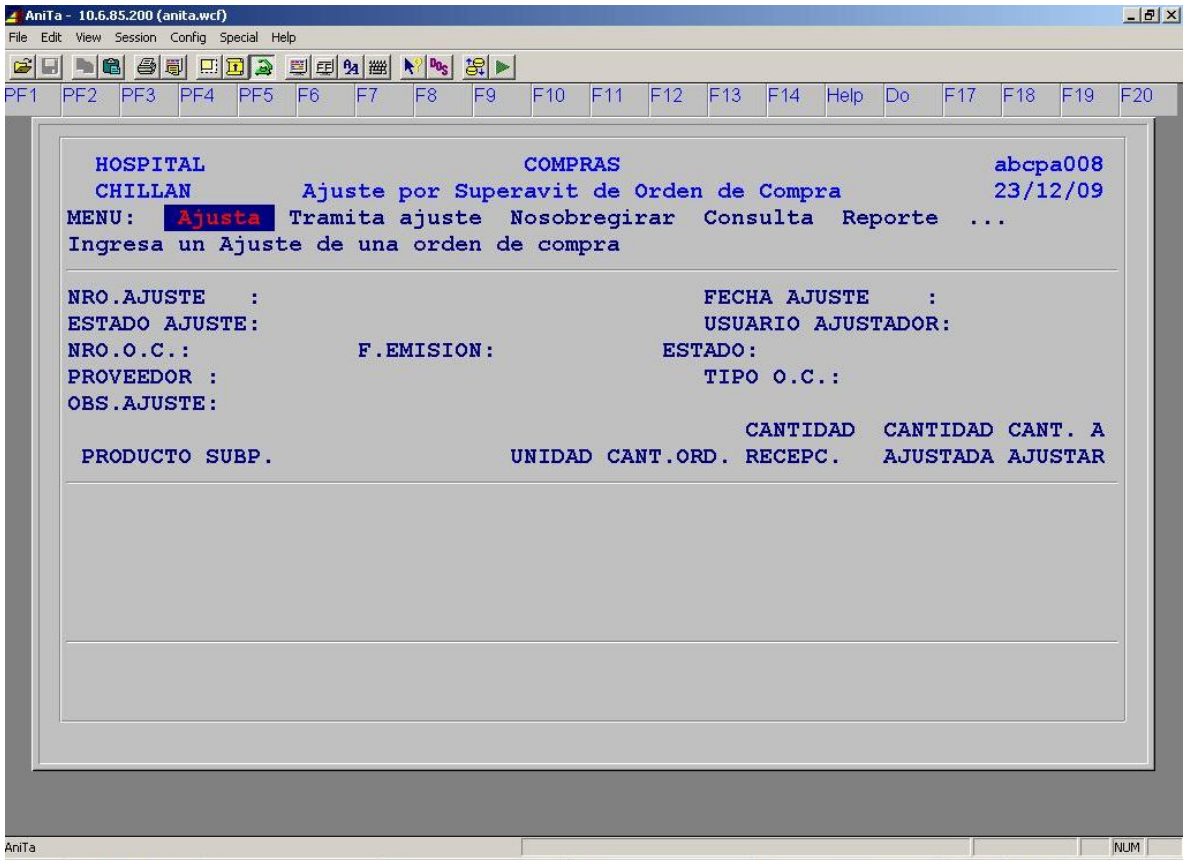

Figura 18: Menú Ajuste por Superávit de Orden de Compra

En la opción ajustar, se ingresa la orden de compra a ajustar y aparecen todos los datos asociadas a la orden de compra indicada. Al mostrar el detalle del producto se podrá modificar la cantidad del mismo para el ajuste. Posterior a esto se debe seleccionar la opción trámite contable para enviar el ajuste a Contabilidad para su aprobación.

C.2. Ajuste por Déficit

Esta función ajusta una Orden de Compra que llegó con menor cantidad a la solicitada. En este proceso se genera una Orden de Anulación por la cantidad de Productos que llegaron de menos. Se ingresa la Orden de Compra y aparecen todos los datos asociados a la Orden de Compra y en la columna Cantidad por Ajustar se ingresa la cantidad a ajustar. Una vez confirmada se genera la Orden de Anulación correspondiente.

La pantalla es la siguiente:

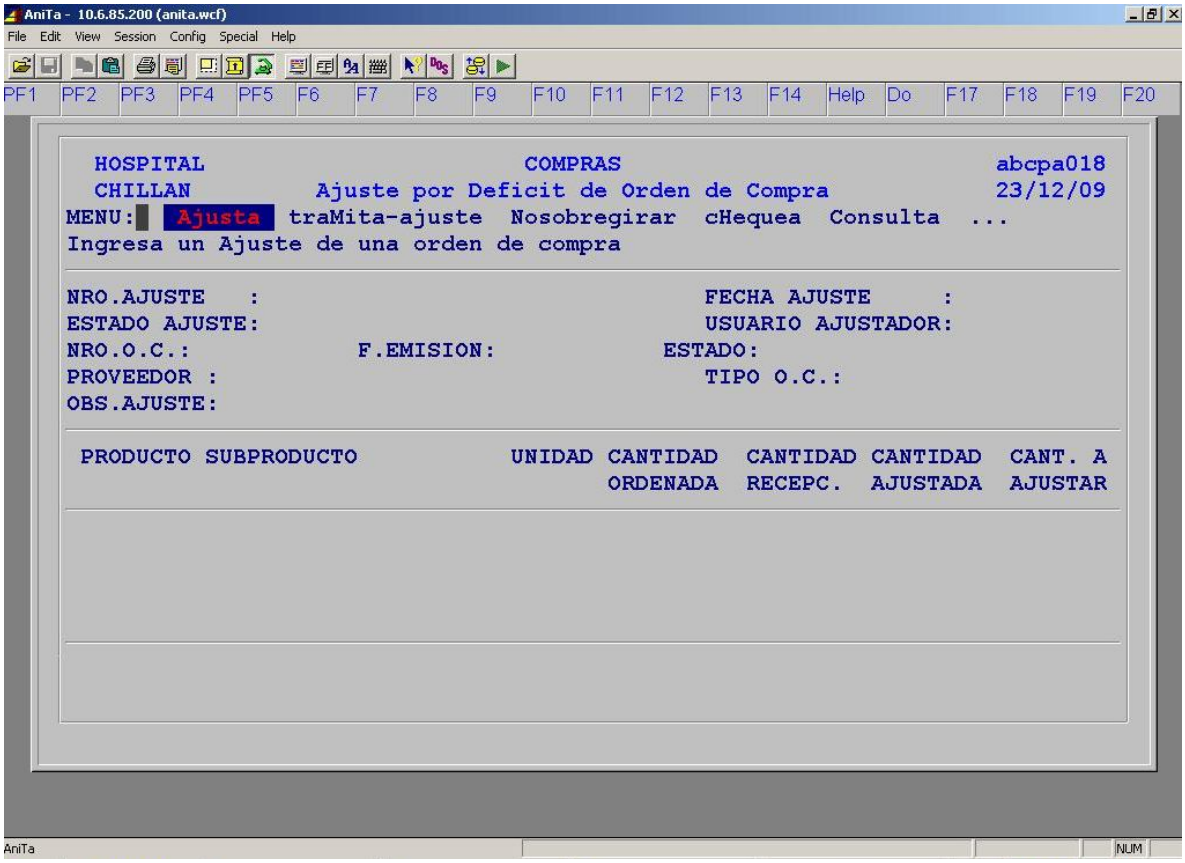

Figura 19: Menú Ajuste por Déficit de Orden de Compra

Una vez generada la Orden de Anulación se debe enviar Contabilidad para su aprobación.

C.3. Anulación de Orden de compra

Esta función anula una Orden de Compra en su totalidad siempre cuando la orden de compra no tenga ningún producto recepcionado parcial o totalmente.

En la opción Consulta se ingresa la Orden de Compra a anular. Una vez que se tenga la Orden de Compra, se procede a ejecutar la opción Anular. Esta anulación se envía a contabilidad para poder revertir el presupuesto asociado al centro de costo.

La pantalla es la siguiente:

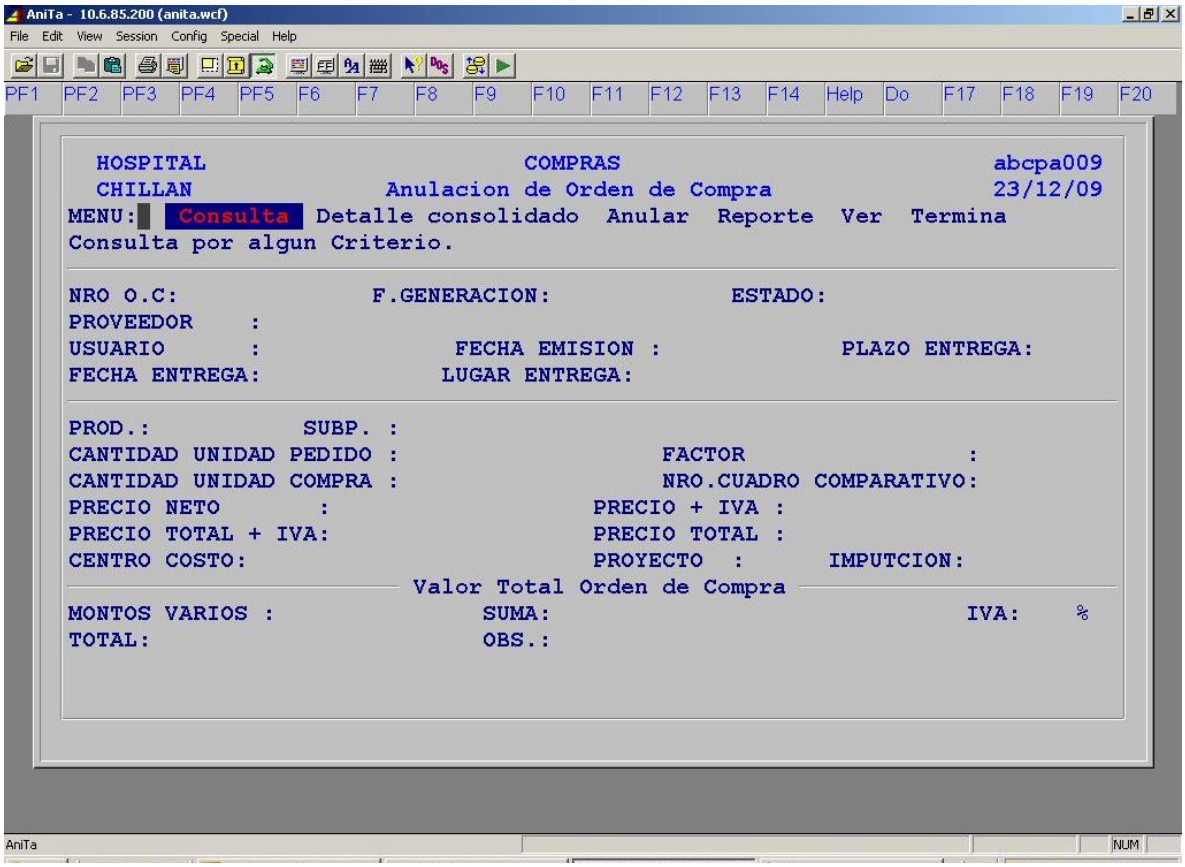

Figura 20: Menú Anulación de Orden de Compra

C.4. Consulta Ajustes Órdenes de Compra por Periodo

Esta función permite consultar por todos los ajustes por superávit y déficit realizados en el sistema dentro de un periodo determinado.

D. Histórico de Compras

La opción Histórico de Compras provee una serie de opciones que permiten consultar bajo diferentes criterios y en un periodo determinado todas las Órdenes de Compras emitidas por el sistema.

D.1. Órdenes de Compra por Período y Estado

Esta función permite consultar por todas las Órdenes de Compra en un Estado en particular para un periodo determinado.

D.2. Órdenes de Compra por Período y Proveedor

Esta función permite consultar por todas las Órdenes de Compra que estén dentro de un periodo determinado y para un proveedor en particular.

D.3. Órdenes de Compra por Período y Producto

Esta función permite consultar dado un subproducto y periodo, las cantidades totales compradas para un subproducto a los diferentes proveedores y el monto total que suman dichas compras.

D.4. Órdenes de Compra por Período y Proyecto

Esta función permite consultar por todas las Órdenes de Compra efectuadas para un proyecto en particular y un periodo determinado.

D.5. Órdenes de Compra por Período y Convenio

Esta función permite consultar por todas las Órdenes de Compra efectuadas para un convenio en particular y un periodo determinado.

D.6. Órdenes por período e imputaciones

Esta función permite consultar por todas las Órdenes de Compra para una imputación contable específica dentro de un periodo determinado.

D.7. Órdenes por Periodo

Esta función permite consultar por todas las Órdenes de Compra realizadas dentro de un periodo determinado.

D.8. Estratificación de Compras

Esta función permite consultar por todos los productos que fueron comprados dentro de un periodo, estableciendo una clasificación desde el mayor a menor monto comprado.

E. Clasificación ABC

Provee las opciones relacionadas con los dos tipos de clasificación que son llevadas para los productos, una de ellas la clasificación ABC y la otra la clasificación VEN (Vitales-Esenciales-No Vitales) éste último para los productos de farmacia.

ABC, Clasificación que se le da a los productos según costo de adquisición anual. Esta clasificación es realizada por un proceso automático dentro del sistema.

- **A** clasificación A mayor costo
- **B** clasificación B
- **C** clasificación C menor costo

E.1. Mantenedor Rangos ABC

Esta función permite asignar para el rango C y B el Monto tope por el cual los productos se considerarán clasificados en A, B o C, es decir, el monto asignado a C, considerará que todos los productos cuyo costo de adquisición (considerando un año) es menor o igual al monto asignado a C se clasificará en la categoría C, sino se verificará contra el rango definido para B. Los montos superiores a B serán considerados clasificación A.

La definición de estas 2 cotas es requisito para ejecutar el proceso que lleva a cabo la clasificación automática.

E.2. Clasificación Automática ABC

Esta función permite clasificar todo el maestro de productos bajo las categorías A, B o C. Se debe indicar el año de la consulta y el sistema ejecutará la clasificación.

E.3. Consulta de Productos por Clasificación ABC

Esta función permite consultar por todos los productos clasificados bajo la relación ABC, se deberá indicar el rubro de los productos.

E.4. Consulta de Productos por Clasificación VEN

Esta función permite consultar por todos los productos clasificados bajo la relación VEN (Vitales-Esenciales-No vitales) , se deberá indicar el rubro de los productos.

F. Cierre del Año

Proceso mediante el cual se actualizan los número de documentos de finanzas, imputación y proyecto de Orden de Compra, Ajustes de Órdenes de Compra, Recepción y Devolución a Proveedores como consecuencia del cierre de año de finanzas, la cual anula los documentos pendientes y genera nuevos documentos con cuentas años anteriores.

F.1. Ejecuta Cierre de Año

Este proceso realiza el cierre de año actualizando el número de documento de finanzas interno, imputación y proyecto para los documentos mencionados.

F.2. Consulta Documentos Procesados en Cierre

Esta consulta permite visualizar todos los documentos que fueron actualizados, desplegando su número de documento de finanzas anterior y actual.

2.6.4.5. Bodega

El módulo de Bodega es aquel que permite administrar los stocks en bodega, registrando los diferentes movimientos y eventos entre bodegas y centros de costos. Este módulo tiene 3 grandes submódulo: Recepción, Distribución y Consumo.

Descripción

En este módulo es posible manejar todo lo referente a existencias de los productos, recepciones, salidas, devoluciones, traspasos y todo lo que esté relacionado con el stock de los productos.

Dentro del módulo de Bodega se encuentra el siguiente menú de navegación:

A- Recepción

- A.1- Recepción por Compra
- A.2- Recepción Genérica
- A.3- Calendario de Recepciones
- A.4- Consulta de Recepciones
- A.5- Consulta Recepciones Pendientes

B- Distribución

- B.1- Salida con Solicitud de Compra
- B.2- Salida con Pedido a Bodega de Stock Reservado
- B.3- Salida con Pedido a Bodega de Stock Disponible
- B.4- Salida Genérica
- B.5- Consulta Despachos Pendientes por Bodega
- B.6- Consulta Demanda Insatisfecha por Centro de Costo
- B.7- Consulta Vencimientos de Productos
- B.8- Consulta Salidas por Periodo

C- Traspasos

- C.1- Traspasos
- C.2- Recepción de Producto en Tránsito
- C.3- Consulta Productos No Recepcionados en Bodega

D- Préstamos

- D.1- Prestamos Hacia / Desde Entidad Externa
- D.2- Devoluciones Hacia / Desde Entidad Externa
- D.3- Consulta Prestamos Pendientes

E- Devoluciones

- E.1- Devoluciones de Abastecimiento - Proveedor
- E.2- Devoluciones de Centro Costo - Abastecimiento
- E.3- Consulta Devoluciones a Proveedores
- E.4- Consulta Devoluciones por Centro de Costo

F- Solicitudes y Entregas Extraordinarias

- F.1- Solicitudes de los Centros de Costo
- F.2- Entregas a los Centros de Costo

G- Control de Existencias

- G.1- Ajuste de Stock
    - G.1.1- Ajuste por Merma
    - G.1.2- Ajuste por Superávit
- G.2- Mantenedor de Partidas
- G.3- Movimientos contables de productos
- G.4- Consultas Existencias
    - G.4.1- Consulta de Stock Global
    - G.4.2- Consulta de existencias por Centro de Costo
    - G.4.3- Consulta de Stock Máximo, Mínimo y Crítico.
    - G.4.4- Consulta Stock por Productos y Movimiento en Tránsito
    - G.4.5- Consulta Existencias Valorizadas
    - G.4.6- Tarjeta Bincard
    - G.4.7- Consulta Productos sin Movimiento

- G.5- Consumo Histórico
    - G.5.1- Consumo de producto
    - G.5.2- Consumo de Centro de Costo
    - G.5.3- Consumo producto por Centro de Costo
    - G.5.4- Consumo Histórico Cons. Inmediato
    - G.5.5- Consumo por Caja Chica, Avance y Anticipos

- H- Seguridad
    - H.1- Bodegas de los Centros de Costo
    - H.2- Permisos de Usuarios a Bodegas

A. Recepción

A.1. Recepción por Compra

Esta función registra el ingreso a Bodega de los productos que han sido solicitados a un Proveedor mediante una Orden de Compra. Permite realizar recepciones parciales o totales de una Orden de Compra, generándose una relación entre ésta y sus recepciones asociadas.

La opción recepción de **Orden Compra**, despliega la siguiente pantalla:

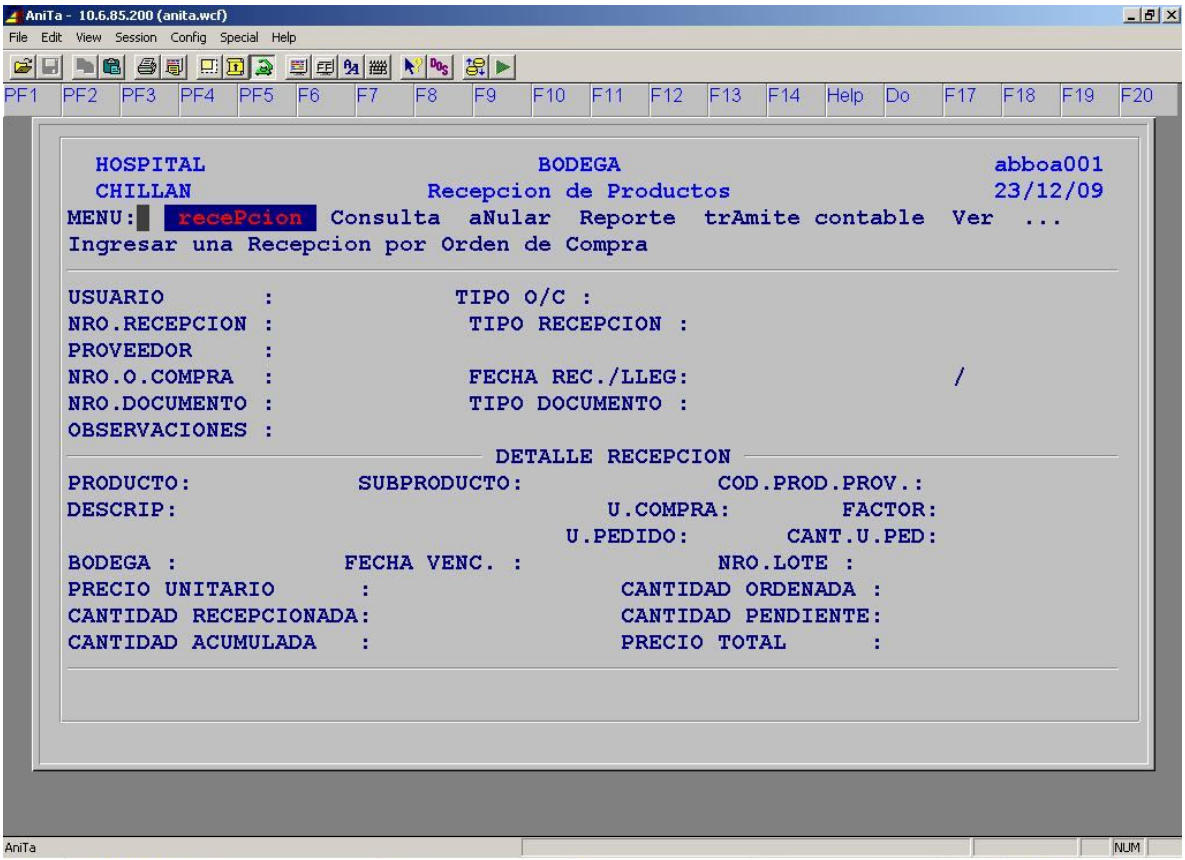

Figura 22: Menú Recepción de Productos

La secuencia de esta operación es la siguiente:

- Primero se selecciona o ingresa la Orden de Compra que se desea recepcionar.
- Se ingresa el número y tipo de documento que respalda la recepción.
- En el detalle de la recepción se despliegan los productos de la orden de compra seleccionada.

- En el campo “CANTIDA RECEPCIONADA”, se indica la cantidad que se está recepcionando del producto, la cual debe ser menor o igual a la cantidad indicada en el campo “Cantidad Pendiente”.
- Una vez se registre la recepción el sistema generará el número de recepción de manera automática.

A.1.2. Recepción Genérica

Esta función registra el ingreso de productos a bodega, que no son sustentados por una Orden de Compra, es decir, que se ingresan con motivo de una donación, transferencia, consumo inmediato o alguna otra razón.

A.1.3. Calendario de Recepciones

Esta función permite consultar por las Órdenes de Compra atrasadas y no atrasadas entregando el número de días de atraso o días faltantes respectivamente.

A.1.4. Consulta de Recepciones

Esta función permite consultar por todas las recepciones realizadas dentro de un periodo determinado.

A.1.5. Consulta Recepciones Pendientes

Esta función permite consultar por todas las recepciones pendientes para una o todas las bodegas.

B. Distribución

B.1. Salida con Solicitud de Compra

Esta función registra las salidas de Bodega de los productos que han sido solicitados por los Centros de Costo, a través de Solicitudes de Compra. Sólo es posible entregar productos asociados de Solicitudes de Compra que tienen al menos uno de sus productos recepcionados parcial o totalmente. Se pueden realizar salidas parciales de una Solicitud de Compra.

La opción **Ingresa**, despliega la siguiente pantalla:

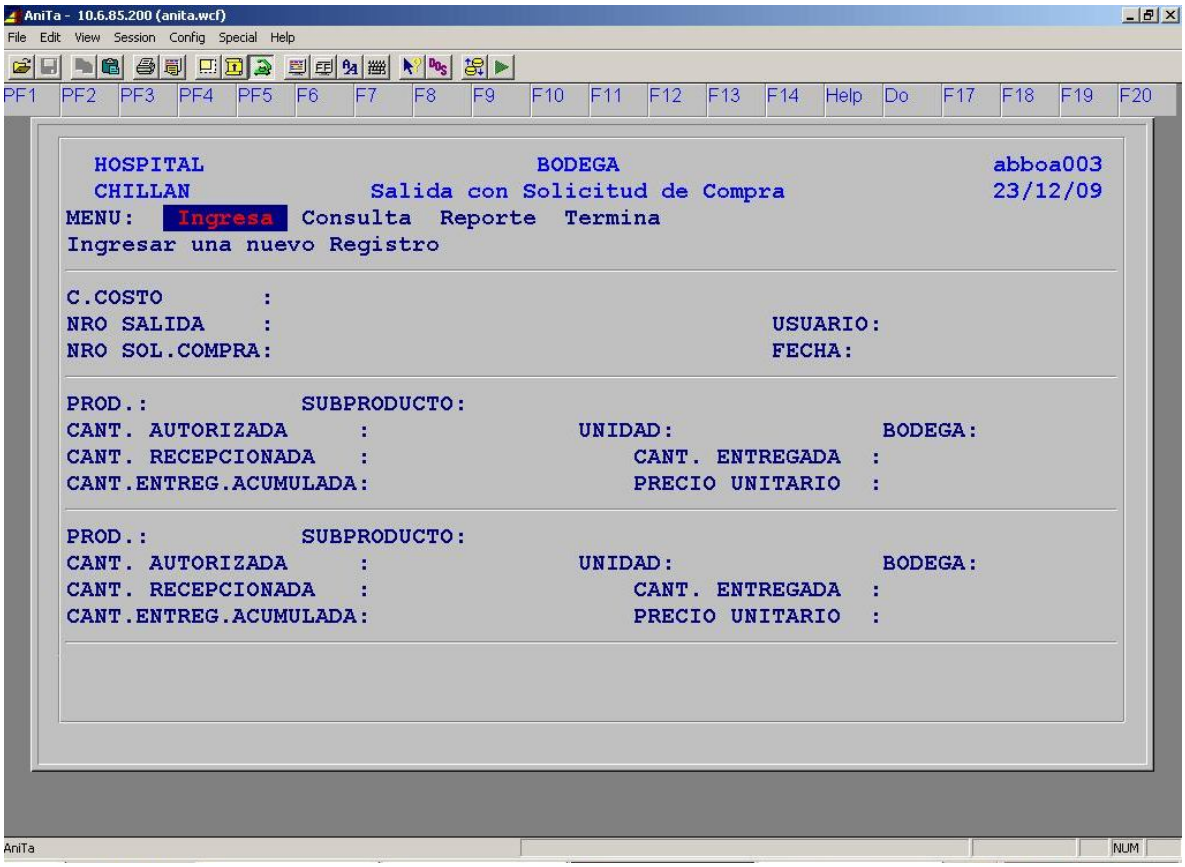

Figura 23: Menú Salida con Solicitud de Compra

La secuencia de esta operación es la siguiente:

- Primero se Ingresa o selecciona el Centro de Costo al que se entregarán los productos.
- Se ingresa el número de la Solicitud de Compra contra la cual se realizará la salida de bodega.
- En el detalle de la salida se ingresa la cantidad a entregar, la cual debe ser menor o igual a la cantidad recepcionada y menor o igual a la cantidad autorizada.
- Una vez guardado se genera un número que la identifica y que se despliega en el campo “NRO SALIDA”.

B.2. Salida con Pedido a Bodega de Stock Reservado

Esta función registra las salidas de los productos que han sido solicitados por medio de un Pedido por Nómina Mensual a Bodega que actúa de acuerdo al Stock Reservado del Centro de Costo que solicita los productos. Para realizar esta función, la secuencia de operación es necesario ejecutar las opciones: Solicita, Visa, Autoriza, Entrega.

B.3. Salida con Pedido a Bodega de Stock Disponible

Esta función registra las salidas de los productos que han sido solicitados por medio de un Pedido por Nómina Mensual a Bodega y actúa de acuerdo al Stock Disponible en Bodega. Para realizar esta función, la secuencia de operación es ejecutar las opciones: Solicita, Visa, Autoriza, Entrega.

B.4. Salida Genérica

Esta función permite realizar salidas de productos desde una bodega, cuya salida rebaja el stock disponible del producto.

La pantalla de esta opción es la siguiente:

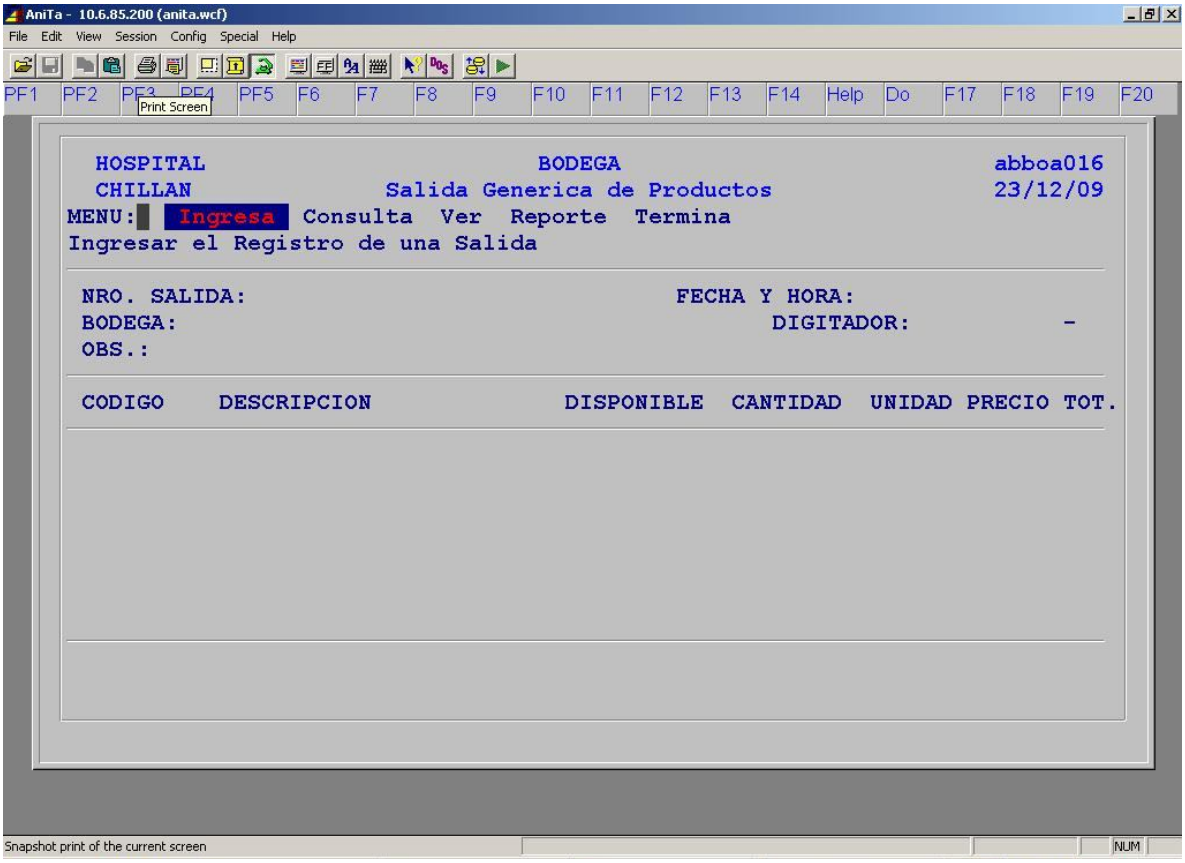

Figura 24: Menú Salida Genérica de Productos

Algunos de los campos son:

- **Número de Salida,** corresponde a la identificación de la salida de productos.
- **Bodega,** código de la bodega de donde se rebajará el stock.
- **Digitador,** código del usuario que está realizando la salida.
- **Código,** es el código que se maneja internamente de los productos.
- **Disponible,** es la cantidad disponible del producto en bodega.
- **Cantidad,** corresponde al número de unidades que se va a rebajar.

B.5. Consulta Despachos Pendientes por Bodega

Esta consulta permite visualizar todos los despachos que se encuentran pendientes para las bodegas.

B.6. Consulta Demanda Insatisfecha por Centro de Costo

Consulta que proporciona información resumiendo lo solicitado versus lo entregado a un centro de costo en particular.

B.7. Consulta Vencimientos de Productos

Este proceso permite ejecutar una consulta para una o todas las bodegas con las fechas de vencimiento de las partidas que cumplan estar en el periodo especificado. La información se entrega ordenada por fecha de vencimiento.

B.8. Consulta Salidas por Periodo

Este proceso permite consultar por todas las salidas de productos que han ocurrido dentro de un periodo determinado y para las bodegas.

C. Traspasos

C.1. Traspasos

Este proceso permite realizar movimientos de stock entre bodegas, en el detalle de la pantalla se deben ingresar los productos y las cantidades a traspasar. Del mismo modo se puede anular un traspaso.

Se requiere conocer la bodega de origen y de destino, además de los productos a traspasar.

C.2. Recepción de Producto en Tránsito

Este proceso permite realizar recepciones de productos enviados por una bodega.

C.3. Consulta Productos no Recepcionados en Bodega

Esta función permite consultar para una bodega y un periodo determinado todos los traspasos no recepcionados en la bodega destino.

D. Préstamos

D.1. Prestamos Hacia / Desde Entidad Externa

Registra los préstamos que se realizan desde el Servicio a una entidad externa o bien los préstamos que una entidad externa le hace al Servicio.

La pantalla de esta opción es la siguiente:

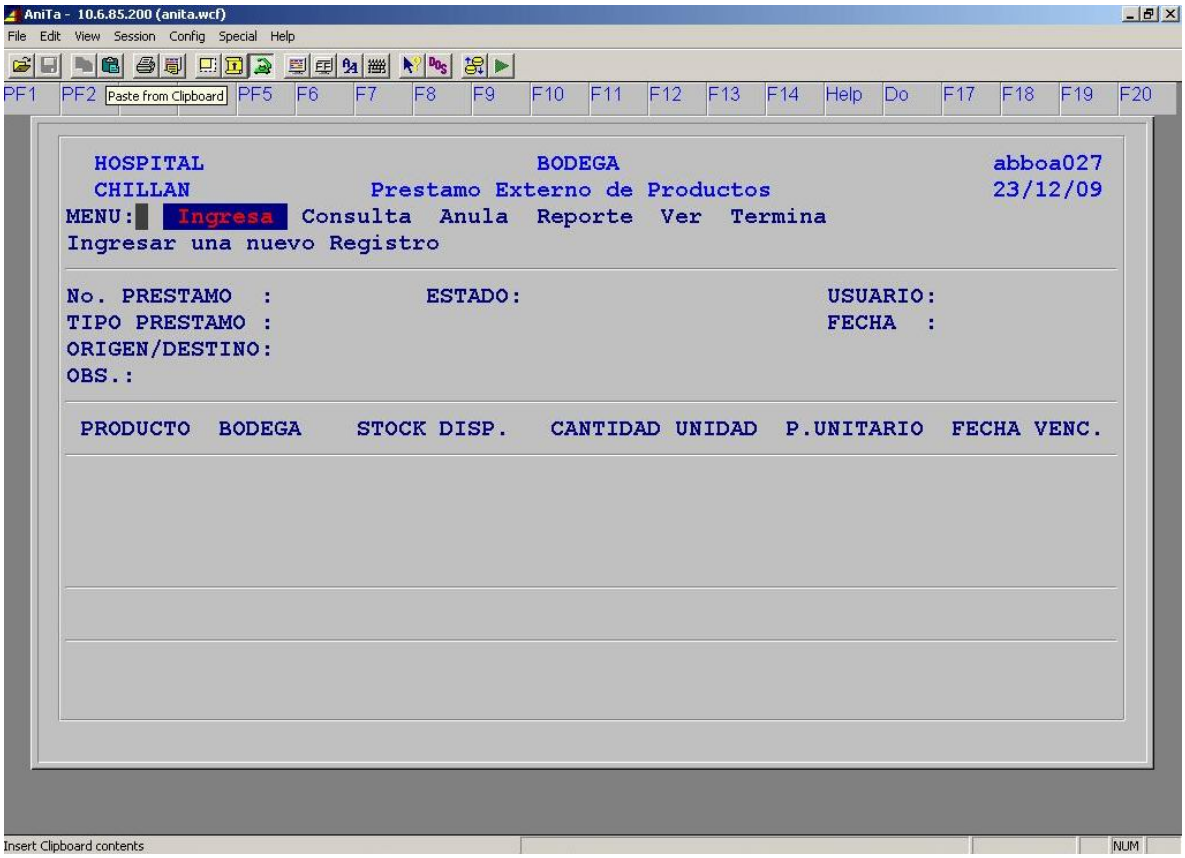

Figura 25: Menú Préstamo Externo de Productos

La opción ingresa requiere de los siguientes datos:

- **Número Préstamo,** es un número único que identifica al préstamo y es asignado por el sistema.
- **Estado,** indica el estado del pedido inicialmente se encuentra pendiente.
- **Usuario,** código del usuario que esta registrando el préstamo.
- **Tipo Préstamo,** este puede ser prestar o recibir préstamo.

- **Producto,** se indicará el producto a prestar o recibir.

- **Bodega,** se indica la bodega a la cual se le realizará la rebaja.

- **Cantidad,** se indica número de productos que se presta o se recibe.

Además cuenta con opciones de consulta y reporte.

D.2. Devoluciones Hacia / Desde Entidad Externa

Registra las devoluciones que realizan las entidades externas al Servicio o viceversa sobre préstamos pendientes.

D.3. Consulta Prestamos Pendientes

Esta función permite consultar por todos los préstamos pendientes a la fecha por diferentes criterios.

E. Devoluciones

E.1. Devoluciones de Abastecimiento – Proveedor

Esta función permite a Abastecimiento registrar una devolución de productos a los proveedores basada en una recepción total o parcial de una Orden de Compra.

La pantalla de la opción es la siguiente:

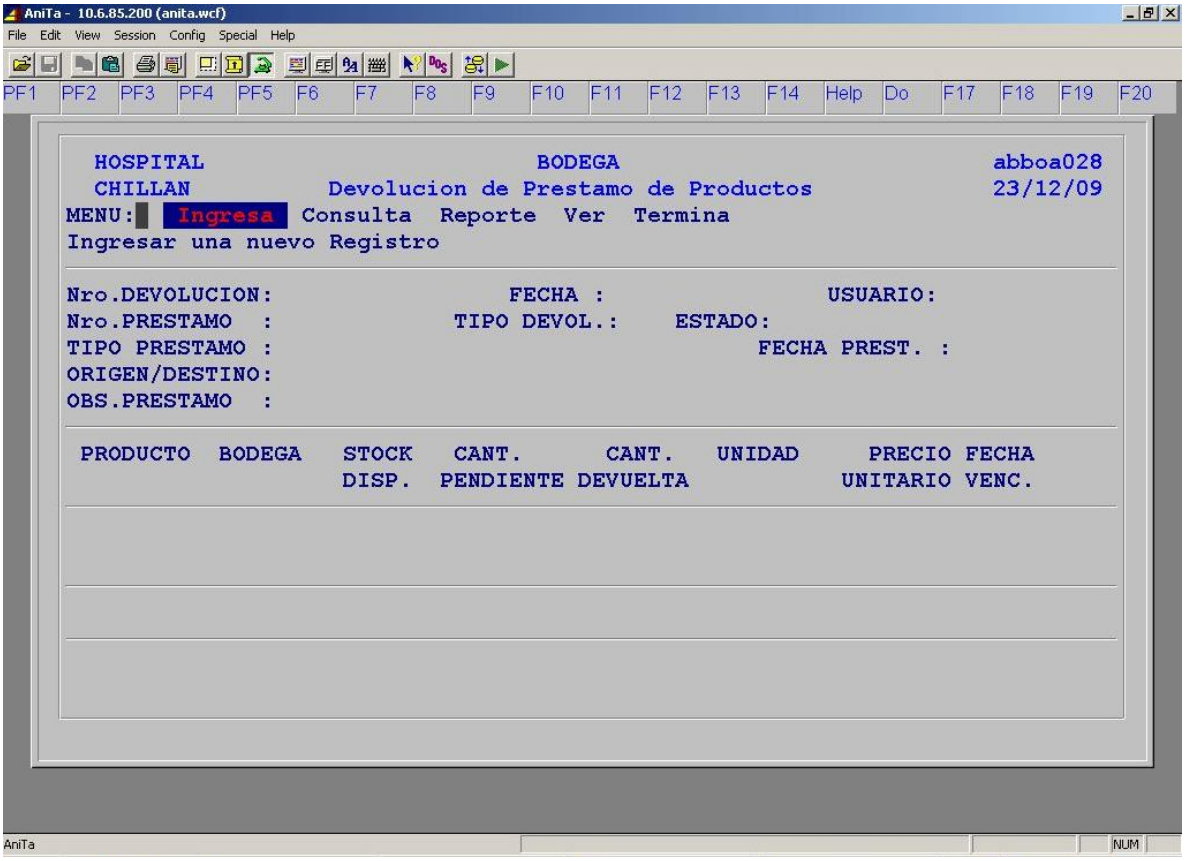

Figura 26: Menú Devoluciones Abastecimiento Proveedor

La opción ingresa devolución requiere de algunos datos como:

- **Número Devolución,** número entregado por el sistema que identifica la devolución.
- **Número de Recepción,** documento asociado por el cual se produce la devolución.
- **Orden de Compra,** número de la orden de compra asociada a la recepción ingresada
- **Estado de la orden de compra,** número que indica el estado en el cual se encuentra la compra.

Además se dispone de opciones como Consulta y reporte.

E.2. Devoluciones de Centro Costo – Abastecimiento

Esta función permite a los Centros de Costo efectuar devolución de productos a Abastecimiento basado en una salida de productos.

E.3. Consulta Devoluciones a Proveedores

Permite consultar por todas las devoluciones realizadas dentro de un periodo determinado para uno o todos los proveedores.

E.4. Consulta Devoluciones de los Centros de Costo

Permite consultar por todas las devoluciones realizadas dentro de un periodo determinado para uno o todos los Centros de Costo.

F. Solicitudes y Entregas Extraordinarias

F.1. Solicitudes de los Centros de Costo

Función que permite solicitar a Abastecimiento de acuerdo a su stock disponible, requerimientos de productos fuera del programa de compras.

La pantalla de la opción ingresar es la siguiente:

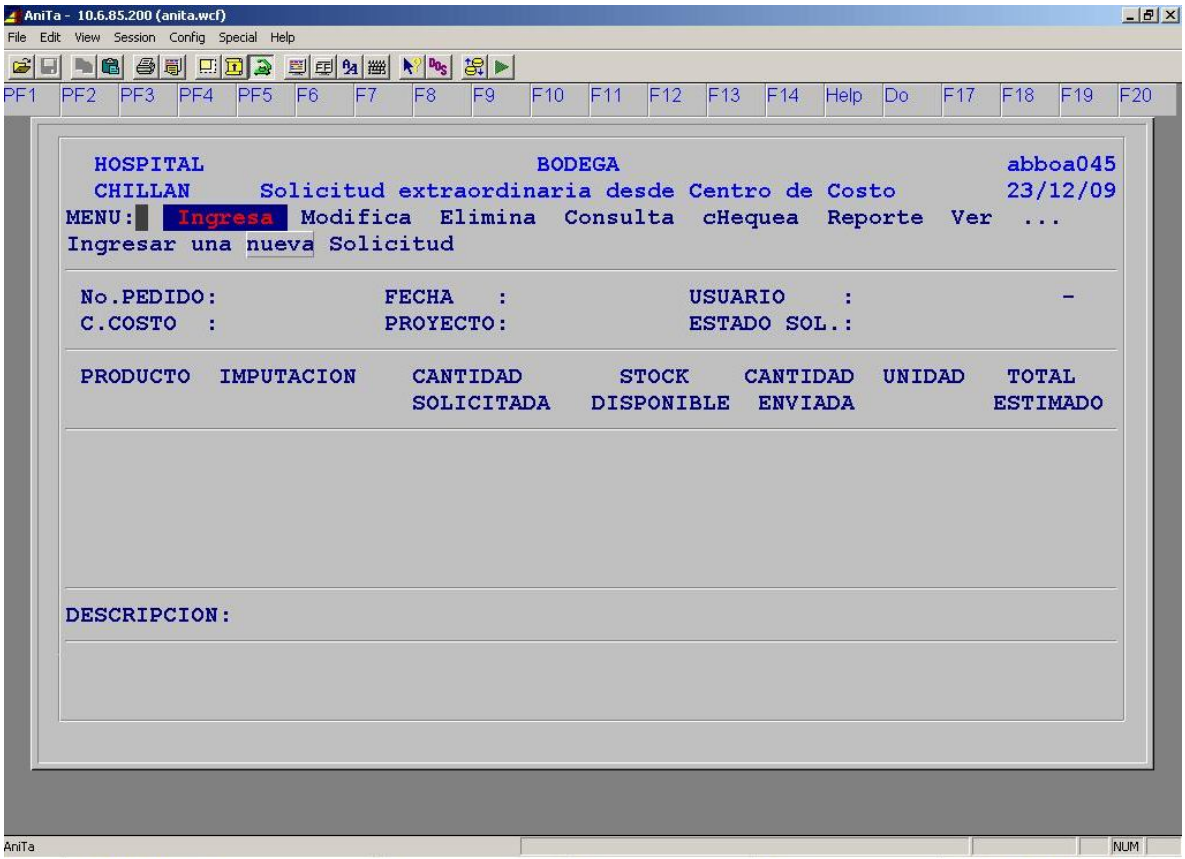

Figura 27: Menú Solicitud Extraordinaria desde Centro de Costo

En esta opción requiere de algunos datos como:

- **Número de Pedido,** este número único es asignado por el sistema e identifica la solicitud.
- **Centro de Costo,** se indica el centro de costos que solicita.
- **Estado de Solicitud,** inicialmente en estado de solicitud.

Se requerirá además datos de los productos y cantidades a solicitar.

Se cuenta también con opciones, de modificación y eliminación de solicitudes en estado "Solicitada", consulta, reporte y chequea (verificando el presupuesto para el centro de costo).

F.2. Entregas a los Centros de Costo

Este proceso permite realizar las autorizaciones y entregas de productos a los centros de costo en base a las solicitudes extraordinarias generadas.

G. Control de Existencias

G.1. Ajuste de Stock

G.1.1. Ajuste por Merma

Esta función permite registrar las pérdidas o mermas de las existencias de productos. Su operación reduce el stock disponible del producto que ha sufrido la baja.

G.1.2. Ajuste por Superávit

Esta función permite registrar los excedentes de las existencias de productos. Su operación incrementa el stock disponible del producto que ha tenido el superávit.

G.2. Mantenedor de Partidas

Esta función permite consultar o modificar la estructura interna de almacenamiento de stock, pudiendo modificar las fechas de vencimiento y fecha de entrada de las partidas.

G.3. Movimientos contables de productos

Esta función permite efectuar un traspaso de productos entre Centros de Costos, provocando un cambio de dueño de la partida y por ende descomprometiendo el

presupuesto del que realiza el traspaso, y comprometiendo presupuesto del que recibe el traspaso, previo a la aceptación del movimiento contable desde Finanzas.

G.4. Consultas Existencias

G.4.1. Consulta de Stock Global

Esta función permite consultar el stock de existencias de productos en una o más bodegas.

G.4.2. Consulta de existencias por Centro de Costo

Esta función permite consultar las existencias de productos agrupados por Centro de Costo.

G.4.3. Consulta de Stock Máximo, Mínimo y Crítico

Consulta por tipo de Stock, el cual puede ser máximo, mínimo, crítico, agrupados por rubro.

G.4.4. Consulta Stock por Productos y sus Movimientos en Tránsito

Esta consulta permite conocer la cantidad de stock disponible y reservado en existencia del producto así como el stock máximo, mínimo y critico fijado para el producto. También nos indica la cantidad de productos pendientes por órdenes de compra enviadas a proveedores que no han sido recepcionadas o se han recepcionado en forma parcial, y las solicitudes de compra extraordinarias hechas por los centros de costos sobre el disponible.

G.4.5. Consulta Existencias Valorizadas

La consulta se puede hacer por precio máximo, promedio o último precio de los productos en una bodega determinada o todas las bodegas.

G.4.6. Tarjeta Bincard

Esta función permite consultar por todas las entradas y salidas que se han realizado para un producto y bodega especifica dentro de un periodo determinado.

G.4.7. Consulta Productos sin Movimiento

Esta función permite consultar por todos los productos que no presentan movimiento en un periodo determinado, es decir, compras, recepciones, devoluciones, traspasos, préstamos y ajustes.

G.5. Consumo Histórico

Proporciona una serie de consultas orientadas al consumo de los productos entregada por diversos criterios.

G.5.1. Consumo de Producto

Esta función permite consultar el consumo para los productos que se encuentran bajo un rubro específico y para un período determinado.

G.5.2. Consumo de Centro de Costo

Esta función permite consultar el consumo de un Centro de Costo en un período determinado.

G.5.3. Consumo producto por Centro de Costo

Esta función permite consultar el consumo de un producto de un Centro de Costo en un período determinado.

G.5.4. Consumo Histórico Consumo Inmediato

Esta función permite consultar por el consumo de productos que fueron comprados a través de consumo inmediato.

H. Seguridad

H.1. Bodegas de los Centros de Costos

Este proceso permite asignarle bodegas a los Centros de Costo.

H.2. Permisos de Usuarios a Bodegas

En esta función es posible asignar a los usuarios los distintos permisos que van a tener en las bodegas que ellos tengan asignadas.

2.6.4.6. Programación de Compras

El Módulo Programación de Compras se encarga de apoyar las funciones relacionadas con la programación detallada de las compras de los Centros de Costo y su consolidación. Para establecer el Programa, los Centros de Costo deben elaborar las Solicitudes de Programa para cada mes y posteriormente en Abastecimiento se consolidan para obtener el Programa Anual de Compras. Se proporciona la funcionalidad de Ajuste al Programa que permite modificar las cantidades programadas por lo Centros de Costo para luego obtener el programa definitivo, a partir del cual se realizan la Nóminas Mensuales de Pedidos.

Descripción

En este módulo es posible realizar los programas de compras tanto mensual como anual, y en base a esto poder realizar consolidaciones y resúmenes, los cuales van a permitir interactuar con otros módulos como son bodega, compras, etc.

El menú principal del módulo de Programación de Compras es el siguiente:

A- Solicitud Programa Compras

B- Consolidación Programa Compras

- B.1- Consolidación por Centro de Costo
- B.2- Consolidación Global
- B.3- Resumen Ejecutivo
    - B.3.1- Resumen Proyecto
    - B.3.2- Resumen Rubro

C- Ajuste a las Solicitudes de Programa

D- Consultas al Programa de Compras

- D.1- Solicitudes de programa de compras
- D.2- Cantidad producto programada por mes
- D.3- Valorización producto programado por mes
- D.4- Valorización programa por Centro de Costo
- D.5- Cantidad y valorización producto programado
- D.6- Valorización programa por rubro

E- Calendario de Pedidos-Entrega

- E.1- Calendario por Mes
- E.2- Calendario por Centro de Costo

F- Nomina mensual de Pedidos-Entrega

G- Producto Programados v/s Ejecutado

A. Solicitud Programa de Compras

Este proceso permite registrar las solicitudes de programa para cada mes del año de cada uno de los Centros de Costo. Desde la generación de las solicitudes de programa de cada mes hasta la consolidación del programa anual de cada Centro de Costo.

B. Consolidación Programa Compras

Esta opción permite consolidar las solicitudes de programa por Centro de Costo y centralizar de manera mensual y anual las Solicitudes de Programa de los Centros de Costo a los cuales se les ha consolidado su programa.

C. Ajuste a las Solicitudes de Programa

Esta opción permite modificar las cantidades solicitadas para cada uno de los productos de la solicitud del Programa de Compras para un mes determinado y un Centro de Costo específico.

D. Consultas al Programa de Compras

Esta opción permite realizar diversas consultas a los Programas de Compra, como:

- Por los estados de las solicitudes de programa de los centro de costos.
- La cantidad de un producto a lo largo del año.

E. Calendario de Pedidos – Entregas

Esta opción permite registrar el Calendario de Pedidos-Entrega de los Centros de Costo para todos los meses del año. El calendario se puede ingresar de dos maneras:

- Calendario por Mes.
- Calendario por Centro de Costos (para todo el año).

F. Nómina Mensual de Pedidos-Entrega

Esta opción permite realizar las Nóminas de Pedidos Mensuales de los Centros de Costo a partir del Programa de Compras.

G. Producto Programados v/s Ejecutado

Esta opción permite consultar y comparar los productos respecto de las cantidades programadas versus las ejecutadas (consumidas) por un centro costo de acuerdo a la nómina mensual.

2.6.4.7. Unidad de Producción

El Módulo Unidad de Producción permite que Abastecimiento y Farmacia lleven un control de la elaboración de productos a partir de insumos.

Descripción

Este proceso permite definir la forma de elaboración de los productos creados, las materias primas que lo componen y sus cantidades.

Este módulo presenta el siguiente menú:

A- Unidad de Especificación

B- Unidad de Elaboración

A. Unidad de Especificación

Este proceso permite definir la forma de elaboración de los productos creados, las materias primas que lo componen y sus cantidades.

B. Unidad de Elaboración

Este proceso permite registrar la definición de la elaboración de los productos creados, las materias primas que lo componen y sus cantidades.

2.6.4.8. Inventario

Este módulo es el encargado de la generación y mantenimiento del inventario.

Descripción

El menú del módulo es el siguiente:

A- Bienes

B- Tipo de Bienes

C- Operaciones Financieras

- C.1- Depreciación y Revalorización
- C.2- Parámetro Monto de Control Financiero
- C.3- Tiempos de vida útil

A. Bienes

Esta función permite ejecutar diversas opciones que permiten la mantención de bienes de activo fijo.

B. Tipos de Bienes

Permite definir tipos de bienes. Para ello será necesario ingresar el código del tipo de bien a ingresar, su descripción.

C.1. Depreciación y Revalorización

Esta función permite ejecutar la revalorización y depreciación de los Bienes de Activo Fijo.

C.2. Parámetro Monto de Control Financiero

Esta función permite modificar el monto mínimo de valor de incorporación de un Bien para que tenga control financiero.

C.3. Tiempos de Vida Útil

Esta función permite mantener la tabla de vida útil en años de los Bienes registrados en el Sistema.

2.6.5. Características del Servidor del Sistema ANITA

Las características técnicas del servidor que soporta el sistema ANITA se detallan en la tabla 1. Este servidor es de alta capacidad y cuenta con características superiores en relación a su nivel de confiabilidad y rendimiento.

Este servidor cuenta con 2 procesadores teniendo capacidad disponible para un total de 4, estos procesadores con tecnología de cobre y capa de silicio, permite que sea más confiable. Además cuenta con memoria Chipkill, la cual permite que el servidor siga funcionando aún en la eventualidad de una falla de un banco de memoria RAM.

Además permite la desactivación dinámica del procesador, permite en caso de falla de uno de ellos, reasignando la carga de trabajo a los procesadores restantes asegurando de esta manera una alta disponibilidad del servidor.

A continuación se detalla las características del servidor:

Marca	IBM
Modelo	RS/6000 modelo pSerie 620-6F0, Modelo Tower
Procesador	2 procesadores RS64 IV de 64 bits 750 Mhz Procesador de 64 bits con tecnología de cobre Tecnología silicon on insulator
Capacidad SMP	Soporta 4 procesadores
Procesador de servicio	RAM 2GB, Máxima: 32 GB Tipo de memoria: SIMMs ECC Chipkill. Cache de Nivel 1 Datos/Instrucciones: 128KB/128KB Cache de Nivel 2: 4 MB por Procesador
Tipo de Memoria	Chipkill
Ancho de Banda de Memoria	2,4 GB/seg

Red	1 Puerta Ethernet 10/100 Mbps no integrada
Slots de Expansión	10 Slots PCI, Hot Plug
Entrada/Salida	1 Puerta Paralelo, 4 Puertos Seriales Diskettera 3.5 `` de 1,44 MB CD-ROM
Almacenamiento en discos Fijos	182 GB en 5 discos de Ultra 3 SCSI de 36,4 GB, Discos Hot Swap
Bahías de Almacenamiento	12 Hot Swap
Controlador RAID	1 Controlador Ultra 3 RAID SCSI Memoria Cache de 128 MB con respaldo, Memoria no volátil 4 Canales Ultra3 SCSI
Controladores	2 Controladores SCSI-2 F/W: 1 interno, 1 externo
Unidad de Respaldo	20/40 GB Interna
Consola	Monitor Gráfico Color 15`` IBM
Adaptador de Video	GXT130P
Controlador	Para 128 puertas seriales, PCI, Compatible con los concentradores de Terminales que tiene el servicio de Salud
Fuentes de Poder	Redundantes y Hot Plug
Ventiladores	Redundantes y Hot Plug
Sistema Operativo Incluido	Aix versión 4.3 licencia para usuarios limitados, Incluye TCP/IP, NFS
Sistema Operativo Soportado	Linux
Tipo de Equipo	De Remarketing, proporcionado por IBM
Garantía	1 año on-site
Informix	Las licencias de informix Online 5 que posee el Servicio de Salud Ñuble son válidas para su instalación en este servidor, al igual que los software adicionales de Informix, como Informix 4GL. Estas licencias son las utilizadas en el servidor p620

Tabla 1: Servidor Sistema ANITA

2.6.6. Base de Datos Sistema ANITA

El software administrador de Base de Datos que se encuentra disponible es INFORMIX 4GL de IBM. Este software ofrece grandes ventajas al llevar a cabo numerosas tareas de procesamiento lógico en el servidor (al contrario que los componentes de procedimiento simples almacenados) en un lenguaje enriquecido y depurable que promueve la eficiencia del programador.

Características principales:

- Proporciona funciones de desarrollo rápido y depuración interactiva.
- Ofrece una extensa funcionalidad de generación de informes comerciales.
- Ideal para lógicas intensivas de cálculo y actualización de tipo no visual.
- Las aplicaciones de los clientes abarcan desde programas de procesamiento de transacciones en línea (OLTP, Online Transaction Processing), como los de registro de pedidos, distribución y comerciales, hasta el procesamiento por compartimientos.

Características adicionales:

- Ofrece un elevado rendimiento en el entorno de producción.
- Integra toda la funcionalidad necesaria para crear incluso las aplicaciones más complejas.
- No requiere el uso de ningún lenguaje de tercera generación.
- Permite un mantenimiento fácil de las aplicaciones.
- Basado en el lenguaje SQL estándar.

Sistemas operativos y plataformas de hardware apropiadas

- AIX
- HP-UX
- Linux
- SUN Solaris

2.6.7. Sistema de Costos HERMINDA

Sistema de Costos HERMINDA, basado en el concepto Data Warehousing, es un repositorio de datos de los diferentes sistemas de información con los cuenta el Hospital.
El control de gestión es un proceso por medio del cual los directivos aseguran la obtención y aplicación eficiente y eficaz de los recursos para así lograr los objetivos de la organización.

La utilización de un sistema de control de gestión basado en Centros de Responsabilidad permite dotar a las diferentes unidades clínicas de una mayor capacidad para tomar decisiones en forma oportuna, autonomía de gestión y negociar periódicamente

objetivos y presupuestos con sus responsables. Así como evaluar constantemente los procesos y resultados en la gestión de la Unidad o Servicio.

Dentro de los modelos de ayuda para la toma de decisiones se encuentra el Sistema de Costos HERMINDA, el cual provee la información de los recursos que el Centro de Responsabilidad demanda, requiere y consume en función de su operación, desempeño y compromisos asumidos con el Establecimiento.

El Sistema de Costos HERMINDA nos permite:

- Registrar los costos y gastos en que incurre cada Centro de Responsabilidad.
- Establecer las medidas adecuadas de seguimiento y proponer las soluciones específicas para corregir desviaciones.
- Programar acciones correctoras.
- Implantación de las correcciones.
- Evaluación de la mejora.
- Evaluar el cumplimiento de Compromisos de Gestión.

Ventajas de Implementación:

- Compatible con otros sistemas del HCHM.
- Se ajusta a las necesidades propias del HCHM.
- De fácil manejo y entendimiento.
- El costo de implementación y manutención es menor al beneficio.
- Flexible.

2.6.7.1. Procedimiento de Cargos de ANITA al Sistema HERMINDA

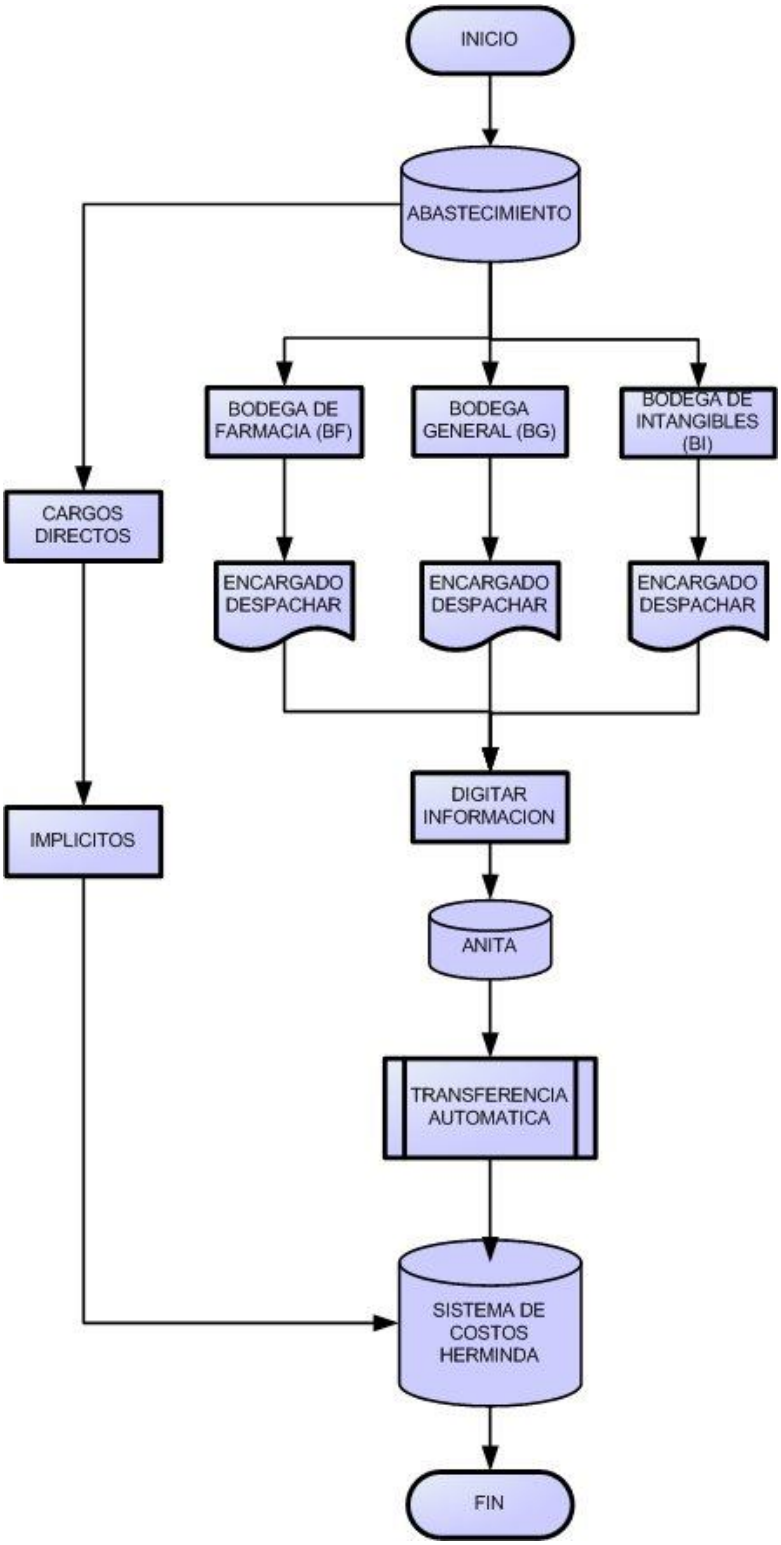

Figura 28: Procedimiento de Cargos de ANITA al Sistema Herminia

Descripción

De la Sección de Abastecimiento dependen tres bodegas, estas son la Bodega de Farmacia, Bodega General y la Bodega de Intangibles. Cada una de ellas posee un encargado de despacho de bodega, en el caso de la Bodega de Intangibles es el jefe de la misma, quienes digitan en el Sistema ANITA las salidas hacia los distintos servicios.

Con este proceso se está alimentando de información el Sistema HERMINDA, este proceso se realiza extrayendo de forma automática la información desde el Sistema ANITA.

Paralelo a esto se cargan al sistema HERMINDA los Cargos Directos, denominados Implícitos, entre ellos están, Fondo Fijo, Luz, Agua, Teléfono, Gastos Menores, Pasajes, Viáticos, Peajes, Gastos en Bencina etc.

Con esto concluye el proceso de Cargos de Abastecimiento al Sistema HERMINDA.

2.6.8. Portal Gubernamental Mercado Público

Mercado Público es la Plataforma de licitaciones de ChileCompra. Es un mercado electrónico para asistir los procesos de contratación entre compradores y proveedores del Estado. Cuenta con un conjunto de funcionalidades que permite la publicación y búsqueda de oportunidades de negocio en el Estado, junto a diversos formularios que soportan cada uno de los pasos de un proceso licitatorio: elaboración de términos de referencia, preguntas y aclaraciones, elaboración y gestión de ofertas, suscripción de órdenes de compra y contratos, calificaciones y reclamos, entre otros.

Mercado Público es una evolución de la plataforma transaccional de Compras Públicas de Chile, que obedece a un crecimiento exponencial de la cantidad de compradores y proveedores desde el año 2003, cuando se inicia la reforma al mercado de las compras públicas de Chile, así como a la sofisticación de las aplicaciones demandadas.

Mercado Público se enmarca dentro del plan bicentenario de la Dirección Chile Compra, denominado Chile Compra 2.0 basado en el Plan Estratégico 2008-2010. Chile Compra 2.0 contempla nuevos proyectos innovadores para el Estado que permitirán fortalecer un modelo que es referente en todo el mundo por la combinación de las políticas

de gestión, normativas, de formación y de tecnología, que ha favorecido el acceso de la pequeña y microempresa, la conectividad en las empresas y la transparencia del sector público.

2.7. Objetivos de la Auditoría

El objetivo de la auditoría Informática a la Sección de Abastecimiento es emitir una opinión independiente y calificada, respecto de la información soportada por los diferentes sistemas de información utilizados dentro de la sección y que apoyan a las diferentes unidades del HCHM. También verificar el buen uso de estos sistemas, según la correcta aplicación de las políticas impuestas por el Ministerio de Salud en materia de seguridad informática. Analizar como se ejecutan los procedimientos desarrollados por el área como es la compra, almacenamiento y distribución de todos los insumos que en la institución se utilizan. Así como también verificar el cumplimiento de las normas internas establecidas y el destino de la información generada.

2.8. Alcance de la Auditoría

La Auditoría se llevará a cabo en la Sección de Abastecimiento del HCHM, donde se abarcarán los procesos de compra, recepción y almacenamiento, distribución que son los encargados de suministrar la información a los sistemas de información que el área utiliza.

Esta auditoría no someterá a evaluación al sistema gubernamental Mercado Público, por tratarse de un sistema cuya administración no recae sobre la institución auditada, como tampoco al sistema PYXIS (Sistema de Dispensación Automática de Insumos) puesto que se encuentra en proceso de puesta en marcha.

Esta auditoría considerará la revisión del desarrollo, puesta en marcha y posteriores modificaciones de los sistemas HERMINDA, ANITA y SISTEMA DE PEDIDOS. Esta auditoría se basará en su funcionamiento actual, sin embargo, se verificará la correcta captura de requerimientos y capacitaciones durante la puesta en marcha de dichos sistemas.

En conclusión esta auditoría estará centrada en emitir una opinión independiente y calificada sobre el funcionamiento actual de los sistemas de información de la Sección de Abastecimiento como además el cumplimiento de la normativa vigente.

2.9. Oportunidad de la Auditoría

La oportunidad de este trabajo práctico de Auditoría Informática se desarrollará en la Sección de Abastecimiento del HCHM, durante el periodo comprendido entre los días 31 de Agosto de 2009 y 30 de Noviembre de 2009.

2.10. Planeación de la Auditoría

La planeación del trabajo de auditoría es considerada como uno de los puntos más importantes dentro del conjunto de actividades que deberán desarrollarse para poder ejecutar de buena forma la actividad de auditoría, es en este punto donde se explicará qué se pretende hacer para poder formarnos una opinión sobre el funcionamiento del sistema y su entorno. Para la realización de esta actividad se llevaron a cabo reuniones con personal de todas las áreas involucradas en el proceso de abastecimiento, como también con el personal encargado del soporte y manutención de los sistemas.

2.10.1. Objeto de la Auditoría

Evaluación de la gestión de la Tecnología de la Información, Sistemas y Procedimientos en la Sección de Abastecimiento del HCHM, para determinar debilidades y fortalezas de la administración de la información.

Las áreas que se someterán a evaluación en esta auditoría son todas las que se relacionan directamente con la Sección de Abastecimiento, tanto en la ejecución como en soporte de los sistemas. Estas áreas son:

- Sección de Abastecimiento.
- Oficina de Ingeniería de Sistemas.
- Área de Soporte de Comunicaciones.

Para el desarrollo de esta auditoría se considerará sólo el Riesgo Operativo en los Sistemas de Información, el cual se puede definir como las deficiencias en los sistemas de información o controles internos que produzcan pérdidas inesperadas. El riesgo esta asociado a errores humanos, a fallas del sistema, procedimientos y controles inadecuados.

2.10.2. Metodología que se utilizará

La metodología a utilizarse para verificar el cumplimiento de los objetivos será la propuesta por ISACA (Information Systems Audit and Control Association), que esta basada en COBIT (Control Objectives for Information and Related Technologies), la cual proporciona un conjunto estructurado de buenas prácticas y metodologías para su aplicación, adaptada al funcionamiento institucional.

COBIT esta basado en la evaluación de riesgos, de manera que partiendo de los riesgos potenciales a los que están sometidas las actividades de la organización. Con lo cual se elabora una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados valores numéricos (metodología de carácter cuantitativo). Estos valores en el caso de las metodologías de análisis de riesgos o de planes de contingencia son datos de probabilidad de ocurrencia o más bien el riesgo de que un evento ocurra. Los que permitirán determinar una serie de objetivos de control de alto nivel que minimicen estos riesgos.

Tanto para el tipo de metodología elegida como para la metodología cualitativa se pueden encontrar una serie de modelos, pero existe consenso en la funcionalidad de la metodología, la cual cuenta con las siguientes etapas[15]:

- Cuestionarios: se realiza entrevista con el fin de evaluar de acuerdo a una escala predeterminada, los distintos riesgos y vulnerabilidades
- Identificación de Riesgos: Posteriormente se clasifican los riesgos de acuerdo a su impacto en la organización.
- Cálculo del Impacto: Se efectúa el cálculo del impacto que va de acuerdo a la probabilidad
- Identificación de medidas y su costo: Se identifican las distintas posibilidades de medidas para minimizar y administrar el riesgo y su costo para la organización.
- Simulaciones: Esta etapa es la más importante, debido al análisis entre las distintas medidas, de acuerdo a consideraciones técnicas y de costo, lo cual determinará el Plan de Medidas de Seguridad.

[15] José María González Zubieta, Auditoría de Tecnologías y Sistemas de Informática, Capítulo 3, Página 63, Año 2008

- Creación de Informes. Es el Plan de Medidas de Seguridad de los Sistemas de Información de la organización, entre lo que se puede mencionar planes de contingencia.

2.10.3. Procedimiento

La Auditoría se basará en la verificación de los Objetivos de Control fijados por las normas COBIT, adaptados a la realidad de la entidad sometida a auditoría informática.

La ausencia de controles internos en materia de Tecnologías de Información en el HCHM impidió realizar un análisis con el detalle deseado. En su lugar se fijaron objetivos de alto nivel de los aspectos relevantes definidos por COBIT.

Además se evaluará el riesgo a los cuales están sometidos los activos de la Sección de Abastecimiento del HCHM y se recomendarán soluciones para la mitigación de su impacto.

2.10.4. Controles a Efectuar

El objetivo de un control es anular un riesgo siguiendo alguna metodología, el objetivo de auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando las políticas de la empresa y los objetivos de la empresa.

Así pues tenemos por ejemplo como objetivos de auditoría de sistemas los siguientes: La información de los sistemas de información deberá estar resguardada de acceso incorrecto y se debe mantener actualizada. Cada una de las transacciones que ocurren en los sistemas es autorizada y es ingresada una sola vez. Los cambios a los programas deben ser debidamente aprobados y probados.

2.11. Objetivos de control que serán evaluados

De los 13 objetivos de control de alto nivel proporcionados por Cobit, en el dominio de Entregar y Dar Soporte (DS), se eligieron y adaptaron a la realidad del HCHM los siguientes:

2.11.1. Seguridad de la información. (DS5 y DS12)

Con el cumplimiento del objetivo DS5 que corresponde a garantizar la seguridad de los sistemas se pretende cumplir con los criterios de información de confidencialidad e integridad y a su vez de manera secundaria con los criterios de disponibilidad, cumplimiento y confiabilidad. Este objetivo busca mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

Mientras que con el Cumplimiento del objetivo DS12 correspondiente a la administración del ambiente físico se pretende cumplir con los criterios de integridad y disponibilidad. Este objetivo busca proteger los activos de cómputo y la información de la institución, minimizando el riesgo de la interrupción del servicio.

2.11.2. Relación con los proveedores externos y clientes (DS2)

Con el Cumplimiento del objetivo DS2 correspondiente a Administración de los servicios a terceros, se busca cumplir con los criterios de efectividad y eficiencia Con esto entregar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.

2.11.3. Planeación de la continuidad del negocio (DS4)

Con el Cumplimiento del objetivo DS4 correspondiente a “Garantizar la continuidad del servicio”, se busca cumplir con los criterios de disponibilidad y efectividad. Alcanzando el mínimo impacto al negocio en caso de una interrupción de servicios de las tecnologías de información.

2.11.4. Capacitación a los usuarios (DS7)

Con el cumplimiento del objetivo DS7 correspondiente a “educar y entrenar a los usuarios”, se busca cumplir con los criterios de efectividad y eficiencia de manera secundaria. Estos requisitos satisfacen el uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos

2.11.5. Administración de datos (DS11)

Con el Cumplimiento del Objetivo DS11 correspondiente a la administración de datos, se busca cumplir con los criterios de integridad y confiabilidad. Estos requisitos buscan Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.

A continuación se presenta un plan detallado de las diferentes actividades que permitirán desarrollar la labor de auditoría según los objetivos previamente establecidos. Este plan esta estructurado de la siguiente manera:

Cada objetivo de control de alto nivel se encuentra detallado en uno o más objetivos de control específicos, los que a su vez se cuentan con una o más actividades de control que permiten verificar su cumplimiento. Además estas actividades de control permiten verificar el nivel de avance o cumplimiento de los compromisos adquiridos con el MINSAL, el cual plantea ciertos estándares en materia de seguridad y conservación de la información.

2.11.1. Seguridad de la información.

2.11.1.1. Objetivo de control: Se han implantado diferentes técnicas y herramientas de seguridad lógicas para restringir el acceso a los sistemas, datos y otros recursos de información relacionados.

Verificar la existencia restricciones en el acceso a los recursos de información y de esta forma poder comprobar la división de obligaciones y tareas, que permitan facilitar aprobaciones en línea como visar las licitaciones y ayudar a lograr los objetivos de control del proceso de adquisiciones. Para alcanzar este objetivo se deben utilizar técnicas y herramientas de seguridad lógicas para definir dichas restricciones de acceso, incluyendo cómo y a quién limitará las atribuciones de cada uno de los perfiles que debiesen existir. En el caso que estas técnicas y herramientas no sean implantadas y configuradas de manera adecuada, las actividades de control del ciclo de negocios no tendrán los efectos para los cuales fueron desarrolladas, y los recursos de información importantes podrán estar expuestos a usos inadecuados, como son la modificación, revelados a personal no autorizado y en ciertos casos pudiendo ser borrados no permitiendo la

disponibilidad de la información, para el correcto desarrollo de los procesos del área.

Actividades de control

I) La dirección revisa y aprueba la implantación y configuración de las técnicas y herramientas de seguridad de la información.

Las técnicas y herramientas referentes a la seguridad de la información, son la base fundamental para el mantenimiento del control sobre el acceso a los recursos de información. Los controles de acceso se pueden implantar en diversos componentes del hardware y software. Al momento de evaluar estas técnicas y herramientas de seguridad de la información, la dirección debería determinar:

- La criticidad de los recursos de información que se protege
- El grado de uso dentro de la entidad
- Los recursos que se necesita implanten y mantengan la herramienta
- La capacidad de identificar y hacer responsables a los usuarios por la actividad que desarrollan en el sistema
- Especificación de los criterios de autenticación
- Identificación y protección de todas las trayectorias de acceso a los recursos de información,
- Los planes del sistema de información.

El considerar estos aspectos garantiza en cierto modo, que los controles de seguridad de la información en el lugar, cumplen con las expectativas de la dirección y con las necesidades de la Sección de Abastecimiento.

II) Las herramientas de seguridad de información implantadas, permiten llevar un control de los errores de acceso y estos son revisados periódicamente, para adoptar medidas correctivas necesarias.

Una herramienta de seguridad efectiva proporciona a la dirección la capacidad para emitir informes de los sistemas, identificar las opciones de

configuración de seguridad y cambios y ayuda a resolver debilidades de seguridad. El sistema debiese tener la capacidad para registrar un historial, que permita la seguridad relativa a eventos tales como intentos de acceso no autorizado y el uso de recursos sensibles. Estos informes se debiesen generar en forma rutinaria y ser revisados de manera oportuna tanto por la dirección y los administradores del sistema o los encargados de la seguridad del mismo. En caso que esto no se aplique usuarios no autorizados podrán tener acceso y modificar los datos sin que sean detectados de manera oportuna.

III) Se modifican las contraseñas predeterminadas por los diseñadores del Sistema.

Los desarrolladores de los sistemas proporcionan perfiles, identificación de usuario y contraseñas, las cuales en primera instancia resultan ser ampliamente conocidas dentro del mundo de la tecnología de la información, como son los 4 ó 5 primeros dígitos del Rut, lo que representa una amenaza importante a la seguridad debido a que la identificación del usuario y las contraseñas son extremadamente obvias, y se encuentran entre las primeras que utilizan los hackers internos o externos para obtener acceso a los sistemas. Además algunas de las identificaciones y combinaciones de contraseñas predeterminadas proporcionan un acceso que puede contener un perfil con amplias atribuciones, como por ejemplo acceso supervisor o de administrador. Esto resulta dañino y compromete los principios fundamentales de todo sistema seguro como son la confidencialidad, integridad, privacidad especialmente tratándose de una institución de salud como lo es el HCHM, que maneja información de carácter relevante para el bienestar de la comunidad.

Para contrarrestar el riesgo de que éstas sean utilizadas de forma maliciosa por el personal o personas externas a la organización, deberían eliminarse o deshabilitarse estos perfiles o deberían cambiarse las contraseñas predeterminadas por el desarrollador, durante la primera sesión que inicie dicho perfil. Exigiendo una composición más robusta.

IV) Se requiere que los usuarios tengan un identificador único de usuarios con el fin de distinguir a un usuario de otro y establecer responsabilidades.

La autenticación de los usuarios sirve para validar al personal que utiliza los sistemas de información. Es la encargada de diferenciar entre un usuario y otro, además de establecer la responsabilidad y atribuciones que tendrá cada uno de estos en el sistema. Los procedimientos inadecuados de autenticación podrían llevar a pérdidas materiales o alteración de datos y un uso inapropiado de los recursos de información.

La dirección debe enfatizar el valor de la información de la entidad, haciendo que la seguridad sea política del HCHM y con esto conseguir que los usuarios sean responsables de las transacciones realizadas utilizando su identificación de usuario.

2.11.1.2. Objetivo de control: Se han implementado restricciones de acceso físico con la finalidad de garantizar que solamente el personal autorizado pueda tener acceso o utilizar los recursos de información.

Los recursos asociados a los sistemas de información del HCHM incluyen hardware, periféricos, dispositivos de almacenamiento de información y documentación de los sistemas de información. El acceso físico a estos recursos da la posibilidad al usuario de ver, usar, malversar o dañar en forma intencional estos recursos. Por estas razones, es que el acceso físico debe estar restringido únicamente al personal autorizado para desempeñar ciertas tareas.

El análisis y evaluación del riesgo indica que este ítem es calificado con un riesgo muy importante (ver Anexo VI, sección 3.1), por el impacto que produciría a los activos de la institución, debiendo tomar medidas para realizar un control efectivo de aquellas actividades, y cambiar los procedimientos que se están realizando de manera errónea o poco segura.

Actividades de control

I) El acceso físico a la sala de servidores es monitoreado y restringido, y es sólo accesible para el personal que trabaja en el área.

Los controles de acceso físico proporcionan la capacidad la dirección de otorgar y negar el acceso físico de individuos a las áreas sensibles. La sala de servidores, las unidades de respaldo en sitio y equipo de comunicación deberán mantenerse en una zona segura que no sea visible a los que no son empleados. Únicamente deberá permitirse el acceso al equipamiento al personal autorizado.
Los controles de acceso físico por lo general debiesen ser aplicables en las siguientes áreas:

- Área de programación, sala de computadoras y terminales
- Cuarto de control de entrada/salida(respaldos) y sala de almacenamiento de dispositivos de respaldo
- Salas con equipamiento que sea portable (impresoras, PC, lectores de código de barras, laptop, entre otros)
- Equipo de telecomunicaciones (módems, teléfonos).

Los controles de acceso físico pueden ser muy eficaces para evitar que personas no autorizadas obtengan acceso a las áreas sensibles, así como también pueden ser vistos como un inconveniente para el personal que necesita tener acceso diariamente. Como en cualquier sistema computacional, debe considerarse la naturaleza de la información y procesamiento del sistema para evaluar el alcance de la seguridad física que se requiere para proteger el hardware y los medios.

Las consecuencias potenciales del debilitamiento de la seguridad física ocasionado por la violación intencional o accidental de las medidas incluyen las siguientes:

- Ingreso no autorizado a áreas sensibles.
- Daño al equipamiento.
- Robo del equipo, propiedad o documentos.

- Copia u observación de la información confidencial y equipos sensibles.
- Revelación pública de la información sensible.

2.11.1.3. Objetivos de control: Todos los recursos de información están sujetos a seguridad física y lógica adecuada.

Todos los recursos importantes de información deben estar sujetos a la seguridad lógica y física adecuada, así como también se debe trabajar en forma coordinada con la seguridad para dichos recursos. En caso que esto no ocurra, las restricciones de acceso que se definen para un recurso podrían hacer que las restricciones de acceso para otro recurso fueran incompatibles. Estas medidas de seguridad deben estar en constante revisión, en la medida de que los sistemas del HCHM tengan cambios y deberán reevaluarse las necesidades de seguridad de información de la entidad para garantizar que sigan siendo efectivas.

Actividades de Control

I) El acceso de usuario está controlado mediante contraseñas u otros mecanismos. Las contraseñas se cambian periódicamente.

Los privilegios de acceso de cada usuario están directamente relacionados con las condiciones que definen la naturaleza del acceso a los recursos, la extensión del acceso y los periodos de tiempo en los que el acceso podría ocurrir. Los desarrolladores de las aplicaciones son responsables de determinar quién debe tener acceso y qué privilegios de acceso se le otorgaran. Al determinar los privilegios de acceso de un usuario, se debe asegurar de que se conserve la división de obligaciones y que se cumplan con los requerimientos laborales.

El acceso a las siguientes categorías de recursos lógicos deberá considerarse en la evaluación:

- Datos
- Código fuente del software de aplicación
- Software de la base de datos

- Software de red
- Base de datos de seguridad

En los casos en los que no estén definidos y establecidos correctamente los privilegios de acceso, la disponibilidad, confidencialidad e integridad de la información podría verse comprometida debido a errores intencionales o no intencionales.

II) Se ha llevado a cabo una evaluación de riesgo, que contempla la evaluación de los recursos de información y evaluación de los niveles de riesgo presente.

Para que la seguridad de la información sea efectiva, el HCHM debe asegurarse de que el análisis de riesgo se lleve a cabo de manera regular, ya que estos pueden cambiar en cualquier momento debido a cambios propios del HCHM, cambios en los reglamentos o leyes ministeriales y los cambios tecnológicos. Este proceso es esencial para asegurarse de que se implanten los programas de seguridad e información, que sean flexibles, efectivos en cuanto a su costo y eficientes con el fin de ayudar a reducir la posibilidad de interrupción del negocio durante largos periodos de tiempo y para asegurarse de que todos los recursos importantes de información hayan sido identificados. Esto puede lograrse mediante la comunicación de la seguridad en toda la entidad, y con esto asegurar que en los casos de seguridad y con el surgimiento de nuevos riesgos sean informados manera oportuna al responsable de seguridad.

2.11.1.4. Objetivos de control: Los programas, datos así como otros recursos de información de la entidad están protegidos contra virus.

Un virus es un programa que impacta de manera importante las operaciones de una entidad al consumir la capacidad de procesamiento de la computadora con las solicitudes de procesamiento del virus. Otros virus pueden tener una intención que sea directamente más maliciosa corromper los archivos de un usuario, volver a formatear la unidad de disco duro de un usuario. Una vez que una computadora de algún usuario se ve infectada con un virus, puede ser muy difícil aislar el virus y erradicarlo, debido a que el virus está diseñado para propagarse a sí mismo y para infectar a otros usuarios y redes. Por lo que los controles de protección contra virus

deben enfocarse por lo general en prevenir la infección y todos los usuarios deben estar conscientes de las guías, normas, procedimientos y políticas antivirus de la entidad. Si dichas normas, procedimientos y políticas no son efectivas, se podría destruir o revelar información sin autorización. Además, es probable que se incurra en gastos innecesarios desperdiciando recursos de procesamiento, el costo de aislar y erradicar el virus y el costo de restaurar o recrear la información perdida.

Actividades de control

I) Se verifica que no haya virus en la información y el software antes de que se cargue en el sistema de la entidad

Todo el software y la información deberá verificarse que no contenga virus antes que se cargue en el sistema de la entidad. De no ser así se deberá incurrir en el costo de aislar y erradicar el virus o restaurar la información perdida por la acción de dicho virus.

II) Se carga un software antivirus en todas las computadoras de la entidad y en cualquier computadora a la que se le permite conectarse con la red las cuales tienen relación con el sistema.

Una vez que la computadora de algún usuario se ha infectado con un virus, puede ser muy difícil aislar el virus y erradicarlo debido a que el virus está diseñado para propagarse a sí mismo e infectar otras redes y estaciones de trabajo del usuario. Por consiguiente, los controles de protección contra virus deberán habitualmente enfocarse en prevenir la infección, y todos los usuarios deberían conocer las políticas, procedimientos, normas y guías antivirus de la entidad. Para lo cual se carga un software antivirus en todas las computadoras de la entidad y en cualquier computadora a la que se le permita conectarse con la red de la entidad. El software antivirus debe explorar en busca de virus al descargar datos o programas, abrir un archivo de datos o ejecutar un programa. Para que sea eficaz, la gerencia debe monitorear el cumplimiento de las políticas. Si dichas políticas, procedimientos, normas y guías no son eficaces, la información podría destruirse y/o revelarse sin autorización.

III) Se requiere que los usuarios actualicen las listas de firmas de virus dentro de su software antivirus y que revisen todos los programas externos y datos antes de descargarlos en sus computadoras.

La amenaza de los virus es constante debido a la aparición de virus nuevos o variantes de manera casi diaria. Aunque algunas variantes pueden poseer firmas "similares" a las de otros virus, otras no, y es por esto que las listas de "firma" del software antivirus se actualizan periódicamente. Todos los usuarios deben contar con las listas mas recientes de firmas de virus del software antivirus que utilizan en sus computadoras y se les debe hacer saber inmediatamente cuando se publican las nuevas listas. Los usuarios deberán actualizar periódicamente sus listas de acuerdo con estas últimas versiones. Sin las listas actualizadas de "firmas de virus", la entidad se arriesga a dañar el software y a perder o corromper la información debido a virus no detectados.

2.11.1.5. Objetivos de control: Los recursos de información se encuentran protegidos contra riesgos ambientales y daños relacionados.

El daño a los recursos de información, incluyendo el hardware, los medios de almacenamiento de información y la documentación de los sistemas de información, puede ser el resultado de diversas causas, incluyendo calor, humo, fuego, humedad, inundación, terremotos e interrupción de la energía eléctrica. Las contramedidas típicas para lidiar con este tipo de amenazas incluyen sistemas de alarma, equipo extintor de incendios, equipos de aire acondicionado, pisos elevados, filtros de aire, suministro de energía continuo (UPS), baterías, generadores y construcción y pisos resistentes a temblores. La naturaleza y el alcance de las contramedidas deberán basarse en la evaluación periódica que la dirección por orden del ministerio hace del impacto que cada amenaza potencial tendría en el negocio.

Actividades de Control

I) La dirección monitorea periódicamente la eficacia de los mecanismos de control ambiental y evalúa el impacto de las amenazas potenciales a los recursos físicos de información.

El principal objetivo de la evaluación del impacto y de la implantación de las contramedidas es asegurarse de que los procesamientos y recursos computacionales críticos queden protegidos contra daño físico en todo momento. Los recursos generalmente identificados incluyen hardware sensible, como son los servidores de red y de equipo principal, así como los dispositivos de almacenamiento que se encuentran en el sitio, manuales importantes y la documentación del sistema. Sin una evaluación del impacto actual y la implantación de los controles adecuados, podría haber un daño innecesario o interrupción de las comunicaciones, procesamiento, hardware. Dicho daño podría ocasionar fallas en los procesos críticos de la entidad si no se adoptan las medidas necesarias que permitan disminuir el riesgo.

II) La dirección proporciona fuentes de energía alternativas como generadores, suministros de energía constantes.

El daño a los recursos de información, incluyendo el hardware computacional y documentación de sistemas de información puede ser ocasionado por una variedad de causas. Un tipo típico de amenaza es la interrupción del suministro eléctrico. Las contramedidas típicas para tratar esta amenaza incluyen los suministros de energía ininterrumpibles, baterías y generadores. La naturaleza y grado de contramedidas deberá basarse en la evaluación periódica de la dirección del impacto de su no implantación en las diferentes áreas.

2.11.2. Relación con los proveedores externos y clientes.

2.11.2.1. Objetivo de control: Verificar que las tareas de compra, recepción y distribución se están llevando a cabo según los manuales de procedimientos exige el ministerio de salud, para las compras.

Las políticas instauradas por el ministerio de salud exigen el cumplimiento de diferentes procedimientos para la compra de insumos, además existe una serie políticas que regulan el almacenamiento y distribución dentro del HCHM. Todas estas actividades anteriormente mencionadas son desarrolladas por la Sección de Abastecimiento, en sus unidades de compra y bodega.

Actividades de control

I) La Sección de Abastecimiento planifica y ejecuta un plan anual de compras según la reglamentación del HCHM.

Para una institución donde se realizan compras de insumos a través de licitaciones, es de vital importancia tener establecido cuales serán las compras que se deberán realizar para el cumplimiento de este plan, debiendo ajustarse según las necesidades que surgen en las diferentes épocas del año, este proceso debe ser desarrollado conforme a la ley Nº 19.886 correspondiente a la Ley de compras públicas y reglamento. Las principales características de esta ley son:

- Introduce transparencia y eficiencia en el mercado de las compras públicas.
- Produce un ahorro significativo para el estado al aumentar la eficiencia, productividad y rapidez de los procesos de compra de los servicios públicos.
- Impulsa la digitalización de los procesos de compra de los organismos públicos con su correspondiente impacto en el comercio electrónico y posicionamiento internacional del país.
- Permite un aumento en las oportunidades de negocio para las empresas o personas naturales.
- Licitación pública como regla general y obligatoria para las adquisiciones iguales o mayores a 1000 UTM.

- Licitación Privada (Previa resolución)

Además determina los requisitos y procedimientos respecto del contrato de suministro y servicio como son garantías, modificación y término anticipado.

II) Se controla la recepción de los insumos y se almacenan según las disposiciones del HCHM.

Cuando las licitaciones son adjudicadas y son enviadas por los diferentes proveedores, estas deben ser recepcionadas por la unidad de bodega, la que debe verificar que estos envíos se encuentren en buen estado y que además correspondan a la cantidad que fue adquirida como además el precio de la licitación coincida.
Una vez que los insumos son decepcionados, estos proceden ser almacenados según línea de producto en sus respectivos estantes.

III) Se monitorea que la distribución de insumos esté acorde a las solicitudes efectuadas por las diferentes unidades clínicas del Hospital.

Existe una serie de reglas que se deben cumplir para llevar a cabo el proceso logístico de la distribución de los insumos dentro del centro hospitalario, que se inicia con la solicitud de una unidad clínica y que concluye cuando el producto es entregado a la unidad clínica requirente.

2.11.3. Planeación de la Continuidad del Negocio

2.11.3.1. Objetivos de control: En caso de desastre, los procesos del HCHM esenciales y los sistemas de información pueden ser recuperados oportunamente.

La planeación de la continuidad del negocio es un proceso de análisis y recolección de información que tiene como resultado una estrategia integral y un plan correspondiente para responder a interrupciones no planeadas. El objetivo fundamental de este proceso es proporcionar disponibilidad oportuna de todos los recursos que sean necesarios para operar los procesos claves a un nivel aceptable para la dirección. En caso de alguna interrupción no planeada de las operaciones

comerciales normales, se aceptarán niveles de servicio inferiores por un período corto de tiempo. El nivel de servicio que será considerado como aceptable y el lapso de tiempo por el cual se aceptará un servicio menor al completo, dependen de lo crítico de las operaciones que allí se realizan, el costo de reemplazar dicho servicio, el costo de la merma y de los objetivos comerciales de la gerencia. Sin embargo, los procesos que operan durante la recuperación de un desastre deben por lo general incorporar actividades de control que garanticen que la información proporcionada por los sistemas de restauración y recuperación es completa, válida, exacta y disponible oportunamente.

Si una entidad no cuenta con un plan de continuidad del negocio viable y completo, la restauración de los procesos comerciales y de los sistemas de información se verá probablemente retrasada y es probable que la entidad incurra en pérdidas financieras innecesarias en caso de alguna emergencia u otra interrupción no planeada.

Actividades de Control.

I) La dirección ha elaborado y aprobado un plan general de continuidad con base en una evaluación del impacto.

La primera fase de la continuidad del negocio es una evaluación del impacto. La evaluación del impacto identifica el impacto financiero (cuantitativo) y operativo (cualitativo) de una función que se encuentre inaccesible o inoperable en la capacidad de la entidad para realizar sus procesos críticos. La evaluación del impacto proporciona las bases para la estrategia de continuidad de la entidad al proporcionar a la dirección una base para clasificar los procesos críticos que serán recuperados en orden prioritario.

Las consecuencias de no contar con planes eficaces de contingencia para una institución como el HCHM pueden incluir:

- La incapacidad de la entidad para continuar con sus funciones.
- Pérdida de ingresos y por tratarse de una entidad ligada a la salud, la pérdida de vidas.
- Multas y sanciones.
- Pérdida del prestigio institucional.

El análisis y evaluación del riesgo indica que este ítem es calificado con un riesgo **poco importante**, dado que existen planes de contingencia que permiten la continuidad del servicio a pesar de la caída de los sistemas.

2.11.4. Capacitación a los usuarios

2.11.4.1. Objetivos de control: Los usuarios reciben una capacitación apropiada y un apoyo continuo.

Los usuarios de los sistemas de información deben estar en constante aprendizaje para garantizar que los sistemas de aplicación funcionen como se pretende y se aprovechen al máximo las prestaciones.

Actividades de control

I) La dirección monitorea el origen y frecuencia de las solicitudes de apoyo para determinar si se debe mejorar la capacitación de los usuarios, los recursos de apoyo y/o la documentación.

Se deberá monitorear por parte de los directivos la razón y frecuencia por la cual existen solicitudes de apoyo, para que de esta forma se pueda identificar las causas y eliminarlas.

Un rastreo inadecuado de problemas puede afectar de manera adversa la disponibilidad, exactitud y confiabilidad general de los sistemas de información. Además de influir en forma errónea a las decisiones que se adopten como medida.

Si la organización implementa una metodología formal de desarrollo de sistemas, esta deberá indicar cómo y cuándo se realizaran las capacitaciones. Esto también ocurre cuando algún software y hardware sufre cambios significativos, los usuarios deberán ser capacitados para asimilar estos cambios, cómo utilizar los nuevos dispositivos y cómo afectan estas modificaciones al usuario. También se requiere la capacitación cuando cambian los procedimientos o las responsabilidades, o cuando el desempeño actual no es el adecuado. Las políticas, procedimientos, normas y guías en relación con el monitoreo de las tendencias y estadísticas de problemas debiesen incluir al menos:

- Técnicas para identificar problemas.
- Definición de las tendencias y estadísticas de problemas.
- Evaluación del impacto comercial de los problemas.
- Directrices que permitan enfocarse en la corrección de las causas, no en los síntomas que entregan los problemas.
- Análisis e implantación de resoluciones.

II) La documentación actual del usuario para los sistemas de información, se encuentra fácilmente disponible para los usuarios.

Para una organización como el HCHM es muy importante contar con una buena documentación de sus sistemas dado que constantemente se ven expuestos a modificaciones legales que implican modificar los sistemas de información existentes. Donde el real valor de la documentación está determinado por su exactitud, oportunidad y perfección. Una buena documentación facilita la adaptación dada por la alta rotación del personal a la cual se ve expuesto la Sección de Abastecimiento y la Oficina de Ingeniería de Sistemas, esta documentación al ser exacta y precisa describe la funciones del sistema de tal manera que resulta ser un apoyo a la continuidad de las operaciones en caso de transferencia de personal clave. Cuando se implante un nuevo sistema o una modificación al sistema se deberá mantener, desarrollar o reemplazar la documentación. De manera general, se requiere el conocimiento de la funcionalidad del sistema para utilizar de manera eficaz el sistema y el uso eficiente depende de este conocimiento funcional. Además, el uso eficaz y eficiente del sistema, por lo general, requiere del conocimiento de los procedimientos del usuario para elaborar, procesar y dar seguimiento a los resultados del procesamiento. Para garantizar la confiabilidad del sistema, el proceso de desarrollo del sistema debe incluir un plan para el diseño, desarrollo que contemple la entrega de la documentación del usuario final. La documentación del usuario deberá proporcionarse en copias impresas o en línea, y deberá ser accesible para todas las partes afectadas. Si esta documentación no es de fácil acceso al usuario, estos podrían utilizar de manera incorrecta o ineficaz los sistemas de información.

2.11.5. Administración de datos

2.11.5.1. Objetivos de control: Respaldo y Restauración.

Consiste en definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

Actividades de control

I) La dirección y los usuarios planean y programan el respaldo y retención de información, así como la cancelación y liberación de los medios cuando ya no se requiere la retención

Es importante que todos los medios que contengan información, especialmente los respaldos, que cuenten con un periodo establecido de retención. Muchos de estos están descritos por las leyes y reglamentos, así como por las necesidades de la entidad. El periodo de retención debe documentarse para garantizar que la información no se destruya o pierda prematuramente. La información que ha pasado su periodo de retención deberá eliminarse y sus medios deberán ser liberados. Si no se siguen los procedimientos, normas y guías de retención y respaldo, la entidad pone en riesgo la disponibilidad de los medios de almacenamiento e información, el cumplimiento de los requerimientos legales y el uso ineficaz de los recursos.

II) Los respaldos se archivan fuera del sitio donde se generaron para minimizar el riesgo de que se pierdan la información.

Los registros importantes se archivan por lo general, haciendo copias de las bases de datos o archivos de datos y conservando estos como respaldos. Es importante que todos los respaldos sean turnados a un lugar fuera del sitio para minimizar el riesgo de que datos importantes puedan perderse. La recuperación de

los datos perdidos podría requerir esfuerzos importantes o ser prácticamente imposible en ciertas situaciones.

Las políticas, procedimientos, normas y guías relacionadas con la rotación fuera de sitio de los respaldos por lo general incluyen:

- Proceso para crear y almacenar respaldos.
- Procedimientos para seleccionar, rastrear y transportar físicamente los medios de respaldo del sitio a unas ubicaciones de almacenaje fuera del sitio.
- Mantenimiento de los inventarios de medios de comunicación para ubicaciones en el sitio y fuera del sitio.
- Planes de rotación fuera del sitio.
- Comunicación de la política de rotación fuera del sitio a todos los usuarios.

III) Todos los medios (cintas, manuales, documentación, etc.) son almacenados en un lugar seguro de ambiente controlado.

Por lo general, los medios removibles contienen información operacional o financiera histórica importante que puede requerirse con fines de recuperación de desastres o referencia; como tales, debe garantizarse que esta información esté disponible para su uso cuando sea necesario. Dentro de los aspectos que se deben considerar esta la ubicación de los medios removibles, es de suma importancia en una situación de recuperación de desastres. Los respaldos deberán ser almacenados en un lugar que no se vea afectado en caso de desastre en el lugar de procesamiento y que se pueda acceder fácilmente para la transferencia de información a cualquier sitio secundario de procesamiento. Por lo tanto, el lugar deberá estar determinado por el plan de reanudación del negocio tomando en consideración los riesgos tratados y la estrategia alterna de procesamiento.

La información contenida en los dispositivos removibles es por lo general sensible, así como esencial para la recuperación del negocio. Únicamente al personal autorizado por la dirección se le deberá permitir el acceso a los dispositivos

removibles. Si los respaldos no son almacenados en un lugar seguro fuera del sitio, El HCHM se podría arriesgar a lo siguiente:

- No disponibilidad de los respaldos de la información y aplicaciones en caso de desastre (donde los respaldos se verán afectados por el mismo evento).
- Retraso en la disponibilidad de los respaldos de información y el sistema en caso de desastre (donde los respaldos estarán muy lejos del sitio de recuperación).
- Revelación de la información sensible.

IV) Los dispositivos removibles son rotulados para permitir su debida identificación.

Cuando se requiere la recuperación de información o aplicación, es de suma importancia asegurarse de que exista un mecanismo en el lugar para establecer qué contienen los medios removibles y con qué periodo o punto en el tiempo se relacionan. Esta identificación puede realizarse mediante el uso de etiquetas físicas en el medio y la identificación lógica que se tiene sobre los mismos medios. Generalmente, estas identificaciones proporcionarán suficiente información para verificar el contenido de los medios, ya sea directamente o a través de un registro de índice para asegurarse de que no se hagan errores en relación con la reutilización o cancelación de los medios. Se deberá tener cuidado para asegurarse de que la suficiente información esté disponible en caso de desastre para asegurarse de que se puedan identificar los respaldos adecuados.

V) En caso de un desastre, el sistema de información pueden recuperarse en un tiempo razonable.

La administración necesita asegurar que la cobertura de seguros adecuada haya sido adquirida y mantenida. Esa cobertura puede incluir: los costos de sustitución del hardware, restauración de bases de datos, responsabilidad, errores y omisiones, desastres naturales, entre otros. La cobertura de seguros podrá ser necesaria para

cumplir con ciertos contratos comerciales como son las licitaciones. La dirección deberá evaluar la necesidad de:

- Documentar el nivel de cobertura actualmente establecido
- Mantener la cobertura que proporcione costo/beneficios adecuados después de considerarse el ambiente de riesgo.
- Conducir un análisis actual de necesidades de seguros.
- Mantener registros adecuados e inventarios de hardware y otros activos importantes que facilitarán las reclamaciones potenciales futuras.

Si no se mantiene una cobertura de seguros adecuada, el HCHM podrá exponerse a costos importantes para recuperar y restaurar las instalaciones, software y otros tipos de activos, en caso de un desastre.

VI) Restablecimiento de la información bajo un ambiente controlado.

La administración necesita asegurar que la información que se encuentra respaldada, podrá ser restituida de forma integra en caso de ocurrir un desastre, para lo cual se deberán realizar pruebas de restauración de los sistemas de información y de su bases de datos que soportan las áreas mas sensibles del hospital, de tal manera que se verifique el buen estado de los medios en los cuales se están llevando a cabo los respaldos, y que estos podrán responder en caso de desastre.

CAPÍTULO III – EJECUCIÓN DE LA AUDITORÍA

3.1 Introducción

En este capítulo se dará a conocer la evaluación de cada uno de objetivos de control establecidos en el capítulo anterior. Dicha evaluación se realizó una vez analizada la información obtenida en el proceso de Auditoría.

La evaluación del proceso de Auditoría se ha llevado a cabo siguiendo la siguiente pauta; Se presenta los controles que forman parte de la Auditoría, estos controles abarcan diferentes aspectos sensibles para el funcionamiento de la sección. Para dar cumplimiento a los controles se presentan diversos objetivos de control que deberán ser satisfechos por las secciones evaluadas. Cada uno de los objetivos de control tiene una serie de actividades de control, dicha actividad de control somete a prueba al objetivo de control relativo. Por cada actividad de control mencionada se detallará el resultado de la evaluación alcanzada, además se complementará la información indicando por cada actividad de control los compromisos asumidos por la secciones evaluadas y el estado actual de dichos compromisos.

Además se dará a conocer la evaluación de riesgos que compromete los activos de la institución.

3.2. Evaluación de Controles

La Evaluación de los controles se realizará siguiendo el orden descrito en el Capítulo II, sección 2.11, donde se describen los objetivos de control del proceso de Auditoría. La estructura es la siguiente:

3.2.1. Seguridad de la información *(ver sección 2.11.1)***.**

3.2.2. Relación con los proveedores externos y clientes *(ver sección 2.11.2).*

3.2.3. Planeación de la continuidad del negocio *(ver sección 2.11.3)***.**

3.2.4. Capacitación a los usuarios *(ver sección 2.11.4)***.**

3.2.5. Administración de datos *(ver sección 2.11.5)***.**

3.2.1. Seguridad de la información

3.2.1.1. Objetivo de control: Se han implantado diferentes técnicas y herramientas de seguridad lógicas para restringir el acceso a los sistemas, datos y otros recursos de información relacionados.

Actividades de control:

I) La dirección revisa y aprueba la implantación y configuración de las técnicas y herramientas de seguridad de la información.

Las técnicas y herramientas utilizadas para dar seguridad a la información, no son controladas por parte de la dirección, esta responsabilidad es delegada en las dos unidades que tienen bajo su supervisión los Sistemas de Información utilizados por la Sección de Abastecimiento. De esta forma la seguridad del Sistema HERMINDA recae en la Oficina de Ingeniería de Sistemas, mientras que la seguridad del sistema ANITA recae sobre el Área de Soporte de Comunicaciones.

Dentro de los compromisos asumidos están:

a) Identificar ámbitos a prohibir y controlar en el acceso a sitios de Internet. Mantener actualizado un listado de sitios Web prohibidos y mantener un listado actualizado de sitios Web controlados.

   Para ello se estableció un plazo límite de implementación de diciembre del 2008, lo que a la fecha se encuentra implementado en un 20%.

   Estado Actual: Se envió un listado de sitios WEB por parte del Ministerio de Salud que debieran bloquearse (por ejemplo: pornografía), pero no se ha establecido una lista de sitios en particular que deben bloquearse. Está pendiente una reunión con los Directivos para establecer dicho listado.

II) Las herramientas de seguridad de información implantadas, permiten llevar un control de los errores de acceso y estos son revisados periódicamente, para adoptar medidas correctivas necesarias.

Tanto el Área de Soporte de Comunicaciones, como la Oficina de Ingeniería de Sistemas no mantienen un control de los errores de acceso a los sistemas que son mantenidos por las respectivas unidades.

El Sistema ANITA registra los movimientos de las licitaciones que contienen errores, pero estos no son monitoreados con frecuencia.

El Sistema HERMINDA por tratarse de un repositorio de datos no cuenta con este tipo de registro, ya que solo permite ver datos y generar reportes, pero no la modificación de la información que este aporta.

Por otra parte los privilegios asociados a cada perfil no son reevaluados periódicamente por alguna comisión, lo que conlleva a que muchos usuarios no puedan desempeñar tareas cotidianas y requieran el apoyo de otros usuarios para la correcta ejecución de algún proceso. Como por ejemplo la emisión de ciertos informes que apoyan la gestión del área.

III) Se modifican las contraseñas predeterminadas por los diseñadores del Sistema.

No existe una política para el cambio de claves, en ambos sistemas se definen los nombres de usuario y contraseñas basadas en el RUT, las cuales son mantenidas en ambos sistemas hasta que un usuario requiera que ésta sea modificada. Por lo que estas contraseñas son conocidas por todos los trabajadores del área respectiva.

IV) Se requiere que los usuarios tengan un identificador único de usuarios con el fin de distinguir a un usuario de otro y establecer responsabilidades.

Existe autenticación única para cada usuario definida según la “normativa para los nombres de usuario”, que permite distinguir quien realiza cada operación en el sistema, por otra parte no existe una asignación correcta o actualizada de los privilegios del personal del área, lo que deriva en que diferentes usuarios conozcan las cuentas de otros, para poder llevar a cabo todas las tareas necesarias para completar algún proceso.

Dentro de los compromisos asumidos están:

a) Establecer la normativa de nombres de usuarios para Sistemas Operativos y Sistemas de Información de tal forma de asegurar uniformidad y unicidad en él. Elaboración y Difusión de Norma de formato de nombre de usuario.

Para el cual se estableció un plazo limite de implementación de noviembre del 2008, lo que a la fecha se encuentra implementado en un 20%.

Estado Actual: Se estableció una normativa para los nombres de usuario para Sistemas Operativos de Red, pero aún no se establece para los Sistemas de Información.

3.2.1.2. Objetivo de control: Se han implementado restricciones de acceso físico con la finalidad de garantizar que solamente el personal autorizado pueda tener acceso o utilizar los recursos de información.

Actividades de control

I) El acceso físico a la sala de servidores es monitoreado y restringido, y es solo accesible para el personal que trabaja en el área.

El acceso físico se encuentra restringido a personal ajeno a la institución, para todas las áreas donde se encuentran los recursos asociados a los Sistemas de Información. Por otra parte el HCHM asumió ciertos compromisos en materia de seguridad con el ministerio de salud.

Dentro de los compromisos asumidos están:

a) Los centros de cómputo de la Dirección de Servicio y el HCHM deberán ubicarse en habitaciones aisladas, con acceso restringido.

Para el cual se estableció un plazo limite de implementación de diciembre del 2008, lo que a la fecha se encuentra implementado en un 100%.

Estado Actual: Las ubicaciones de los Centros de Cómputo se encuentran en áreas aisladas de los establecimientos con acceso poco

transitado, de acceso restringido pues se debe traspasar de 1 a 2 puertas de acceso y/o ambientes diferentes.

b) Las habitaciones donde se ubiquen los Centros de Cómputos de la Dirección de Servicio y el HCHM deberán ser de paredes de concreto por sus cuatro límites.

Para el cual se estableció un plazo limite de implementación de diciembre del 2008, lo que a la fecha se encuentra implementado en un 100%.

Estado Actual: Las paredes de ambos Centros de Cómputo son de concreto en todos sus límites, ubicados en segundos pisos de los edificios, con equipos de control de temperatura ambiental, solo accesibles a través de 1 puerta.

c) Las puertas de acceso a los Centros de Cómputos de la Dirección de Servicio y el HCHM deberán tener sistema de cierre seguro con a lo menos un sistema de chapa de doble giro.

Para el cual se estableció un plazo limite de implementación de marzo del 2009, lo que a la fecha se encuentra implementado en un 50%.

Estado Actual: La puerta de acceso al Centro de Cómputo de la Dirección de Servicio se encuentra con sistema de llave con chapa de doble giro, en el caso del HCHM la puerta de acceso al Centro de Cómputo no tiene chapa de doble giro en ninguna de sus dos puertas, pero existe en una de ellas cierre con candado.

d) Se deberá emitir una Resolución Exenta que nombres los responsables que velarán por el acceso a los Centros de Cómputos de la Dirección de Servicio y el HCHM.

Para el cual se estableció un plazo límite de implementación de marzo del 2009, lo que a la fecha se encuentra no se encuentra implementada.

Estado Actual: No se ha solicitado por parte del encargado de seguridad la emisión de las Resoluciones respectivas con motivo de que los Directivos deben comprometerse con el tema de Seguridad en TIs para lo cual no ha habido la instancia de difusión correspondiente.

e) Para acceder al centro de cómputo se deberá requerir a los menos un sistema de llave física, la cual deberá estar en manos de a lo más 2 personas responsables de permitir el acceso.

Para el cual se estableció un plazo límite de implementación para marzo del 2009, lo que a la fecha no se encuentra implementada.

Estado Actual: No se ha emitido la Resolución Exenta que indica los responsables de los dos juegos de llaves de acceso a los Centros de Cómputo, esto con motivo ya indicado en el ítem anterior.

f) Las personas responsables deberán realizar un registro escrito del ingreso y egreso del personal que accede al centro de cómputo.

Para el cual se estableció un plazo límite de implementación de marzo del 2009, lo que a la fecha se encuentra no se encuentra implementada.

Estado Actual: Se encuentra diseñado el medio de registro a los Centros de Cómputo, pero no se ha realizado la implementación de éste debido a que se requiere realizar una difusión a los involucrados (los responsables de las llaves y clientes del Centro de Cómputo).

El análisis y evaluación del riesgo indica que este ítem es calificado con un riesgo **importante**, por lo debe poner énfasis en medidas de control que mitiguen el impacto en la institución.

3.2.1.3. Objetivo de Control: Todos los recursos de información están sujetos a seguridad física y lógica adecuada.

Actividades de Control

I) El acceso de usuario está controlado mediante contraseñas u otros mecanismos. Las contraseñas se cambian periódicamente.

Cada usuario del HCHM, que requiere el acceso a los Sistemas de Información tanto de la Sección de Abastecimiento como del las otras unidades hospitalarias, cuenta con su respectiva cuenta de usuario y contraseña para acceder a un equipo con acceso a la red, mientras que para los Sistemas de Información como son el Sistema ANITA y el Sistema HERMINDA existen cuentas con diferentes perfiles que son asignados según el cargo que se desempeñe en la unidad.

Otro tipo de acceso a información de los sistemas como es el caso del acceso a la documentación y código fuente, queda exclusivamente reservado para el personal de la Oficina de Ingeniería de Sistemas y el Área de Soporte de Comunicaciones, quienes son los encargados de dar soporte y manutención a Sistema HERMINDA y Sistema ANITA respectivamente.

II) Se ha llevado a cabo una evaluación de riesgo, que contempla la evaluación de los recursos de información y evaluación de los niveles de riesgo presente.

A la fecha no se ha realizado un análisis de riesgo a las diferentes áreas que comprenden el hospital, en materia de seguridad de la información. El personal manifiesta tener un control sobre los riesgos eficaz de acuerdo a los recursos que se destinan a esta materia.

3.2.1.4. Objetivos de Control: Los programas, datos así como otros recursos de información de la entidad están protegidos contra virus.

Actividades de control

I) Se carga un Software antivirus en todas las computadoras de la entidad y en cualquier computadora a la que se le permite conectarse con la red las cuales tienen relación con el sistema.

Todos los equipos con los que cuenta el HCHM poseen Software antivirus licenciado MacAfee, las actualizaciones son puestas a disposición de todo el personal del hospital en un servidor propio. Existen usuarios que cuentan con los permisos necesarios para instalar programas ajenos a la institución para algunos usuarios, que pueden contener algún tipo de Software malicioso que no es detectado por el antivirus, para lo cual es necesario que el equipo sea enviado a manutención al Área de Soporte de Comunicaciones.

Dentro de los compromisos asumidos están:

a) La instalación de Software será exclusivamente de responsabilidad de personal de informática, por lo cual los usuarios no tendrán privilegios para realizar instalación de ningún tipo de Software.
Para el cual se estableció un plazo límite de implementación de Marzo del 2009, lo que a la fecha se encuentra implementado en un 85%.

Estado Actual: Todos los computadores son instalados con permisos avanzados a los usuarios lo cual no les permite la instalación de Software. Salvo algunas excepciones el usuario de un equipo computacional debe solicitar la instalación o autorización de esta al Área de Soporte de Comunicaciones.

b) Todo equipo computacional deberá disponer de un Software para eliminación de malware. Para ello se estableció un plazo límite de implementación de Marzo del 2008, lo que a la fecha se encuentra implementado.

Estado Actual: En la actualidad no se dispone de un Software para eliminación de malware como estándar establecido, en forma muy singular algunos computadores tienen instalados Software de este tipo. Como Servicio de Salud se está gestionando la adquisición de un complemento de McAffe que cumpla dicha función.

II) Se verifica que no haya virus en la información y el Software antes de que se cargue en el sistema de la entidad

Los datos suministrados que permiten la carga de los sistemas, no requiere verificación sobre la existencia de virus, dado que toda la información es digitada en forma manual en el Sistema ANITA. Mientras que el Sistema HERMINDA obtiene la información directamente desde las diferentes bases de datos del HCHM. Por otra parte el funcionamiento del antivirus queda condicionado a las revisiones que desee efectuar libremente cada usuario.

Dentro de los compromisos asumidos están:

a) El antivirus deberá configurarse para que 1 vez a la semana realice una revisión de todos los medios del computador.

Para ello se estableció un plazo límite de implementación de Marzo del 2009, lo que a la fecha se encuentra implementado.

Estado Actual: No se ha establecido la configuración de revisión 1 vez a la semana como un estándar como parte de la instalación.

III) Se requiere que los usuarios actualicen las listas de firmas de virus dentro de su Software antivirus y que revisen todos los programas externos y datos antes de descargarlos en sus computadoras.

Las actualizaciones de antivirus son puestas a disposición para todos los usuarios del HCHM en un servidor propio, las cuales quedan no son actualizadas de manera automática, con lo que cada actualización debe ser realizada por el o los usuarios de un equipo computacional especifico.

Dentro de los compromisos asumidos están:

a) Todo equipo computacional deberá disponer de un Software de contención y eliminación de virus informático, el cual deberá mantenerse actualizado.

Para el cual se estableció un plazo limite de implementación de Octubre del 2008, lo que a la fecha se encuentra en un 97 % de avance.

Estado Actual: Como política del Servicio de Salud hace 4 años se dispone de Antivirus McAffe para todos los equipos, con un sistema de actualización centralizado. A veces por situaciones de conectividad y otras por daño del Sistema Operativo no se encuentran actualizados.

El análisis y evaluación del riesgo indica que este ítem es calificado con un riesgo **poco importante,** por que la mayoría de los compromisos asumidos se han cumplido.

3.2.1.5. Objetivos de Control: Los recursos de información se encuentran protegidos contra riesgos ambientales y daños relacionados.

Actividades de Control

I) La dirección monitorea periódicamente la eficacia de los mecanismos de control ambiental y evalúa el impacto de las amenazas potenciales a los recursos físicos de información.

La responsabilidad de monitorear los mecanismos de control ambiental recae en el Área de Soporte de Comunicaciones y la Oficina de Ingeniería de Sistemas, los servidores que controla y administra el Área de Soporte de Comunicaciones se mantienen en salas donde se controla la temperatura mediante sistemas de aire acondicionado, sin embargo referente a la prevención de siniestros no se consideran medidas de seguridad, ya que no se cuenta con extintores para dicha sala además de contar de una alta cantidad de material combustible dentro de la sala (papeles). A

continuación se detallan los compromisos asumidos en materia de amenazas a los recursos físicos.

Dentro de los compromisos asumidos están:

a) El centro de cómputo debe estar ubicado sobre la cota cero para evitar inundación.

   Para el cual se estableció un plazo límite de implementación de Diciembre del 2008, lo que a la fecha se encuentra en un 100 %.

   Estado Actual: Los dos Centros de Cómputo se encuentran ubicados en un segundo piso.

b) El cableado de red de datos deberá estar protegido adecuadamente. Si la instalación es a la vista deberán protegerse con canaletas Legrand. Si la instalación es entre techo y/o intra muro deberán protegerse con Conduit.

   Para el cual se estableció un plazo limite de implementación de Marzo del 2009, lo que a la fecha se encuentra implementado en un 85%.

   Estado Actual: Con la instalación del Proyecto Carretera 5D se deberá llegar a un cumplimiento total de este indicador. El Servicio de Salud aún se encuentra en proceso de migración por lo cual parte del cableado utilizado en la actualidad corresponde a la red de datos antigua y que en su gran mayoría no cumple la normativa establecida.

c) No se puede fumar, beber, consumir alimentos al interior del centro de cómputo.

   Para el cual se estableció un plazo limite de implementación de Diciembre del 2008, lo que a la fecha se encuentra en un 100 %.

   Estado Actual: Los letreros informativos ya se encuentran diseñados, impresos e instalados en lugares visibles en los Centros de Cómputo.

d) El personal externo debe identificarse claramente y debe quedar registro de las actividades realizadas en el centro de cómputo.
Para el cual se estableció un plazo limite de implementación de Marzo del 2009, lo que a la fecha no se encuentra implementado.
Estado Actual: Con motivo de no estar implementado el Libro de Registro de accesos, aún no se puede iniciar el registro de visitas de personal externo y las actividades que estos realizan.

e) El trabajo por parte de personal externo en los centros de cómputo debe ser monitoreado por un funcionario del Servicio de Salud.
Para el cual se estableció un plazo limite de implementación de Marzo del 2009, lo que a la fecha no se encuentra implementado.
Estado Actual: Al no estar difundido el procedimiento de trabajo sobre el Centro de Cómputo, formalmente este indicador no registra avance. Informalmente la supervisión de personal externo en el Centro de Cómputo siempre se realiza.

f) Los centros de cómputo deben estar alejados de áreas de acceso público de carga y descarga.
Para el cual se estableció un plazo limite de implementación de Diciembre del 2008, lo que a la fecha se encuentra en un 100 %.
Estado Actual: Ambos Centros de Cómputo se encuentran ubicados retirados de zonas de descarga y tránsito y personal ajeno a los establecimientos.

El análisis y evaluación del riesgo indica que este ítem es calificado con un riesgo **poco importante**, sin embargo se deben poner énfasis en las medidas que controlen la presencia de siniestros.

II) La dirección proporciona fuentes de energía alternativas como generadores, suministros de energía constantes.

Actualmente el HCHM cuenta con fuentes de energía alternativas para aquellas áreas que han sido catalogadas como criticas, como es el caso de pabellones y unidades de tratamientos intensivos, referente a los Sistemas de Información de la Sección de Abastecimiento y en general todas las unidades de carácter administrativo no cuentan con un suministro ininterrumpido de energía. Por otro parte los servidores que contienen el Sistema ANITA y el servidor del Sistema HERMINDA cuentan con Sistemas de Alimentación Ininterrumpida (Uninterruptible Power Suply, UPS) que permiten bajar los servidores de esta forma, evitar posibles daños tanto de Hardware como de los datos que allí están contenidos por conceptos de alzas de voltaje. Además en este ámbito el hospital se a comprometido con aplicar 3 ítems de seguridad de información que se detallan a continuación:

Dentro de los compromisos asumidos están:

a) No deben utilizarse en forma permanente zapatillas eléctricas para expandir la capacidad de conexión.

   Para el cual se estableció un plazo limite de implementación de Junio del 2009, lo que a la fecha se encuentra en un 98 %.

   Estado Actual: Todas las instalaciones de Puestos de Trabajo para equipamiento computacional se realizan con sus respectivos enchufes empotrados a la pared, pero ocasionalmente por urgencias se habilitan puestos de trabajo que deben ser implementados y para que funcionen momentáneamente se habilitan con zapatillas eléctricas.

b) Los equipos computacionales clasificados como “críticos” deberán disponer de una UPS independiente**.** Se entenderá como equipos “críticos” aquellos que por los servicios que prestan deben estar disponibles las 24 horas los 7 días de la semana.

Para el cual se estableció un plazo limite de implementación de Junio del 2009, lo que a la fecha se encuentra implementado en un 80 %.

Estado Actual: Todo equipo computacional clasificado como crítico dispone de UPSs de respaldo de energía, se tiene la salvedad de que por desperfecto de un par de UPSs un equipo crítico no se encuentra sustentado con dicho implemento.

c) Se debe elaborar un instructivo de uso correcto de los equipos que utilizan electricidad.

Manual elaborado, difundido y disponible en la intranet

Para el cual se estableció un plazo limite de implementación de Junio del 2009, lo que a la fecha no se encuentra implementado.

Estado Actual: El instructivo se encuentra elaborado, pero no se ha realizado la difusión a los usuarios de equipo computacional y tampoco la publicación de éste.

3.2.2. Relación con los proveedores externos y clientes.

3.2.2.1. Objetivo de control: Verificar que las tareas de compra, recepción y distribución se están llevando a cabo según los manuales de procedimientos exige el ministerio de salud, para las compras.

Los procedimientos destinados a la adquisición, recepción y distribución que son realizados en su totalidad por la Sección de Abastecimiento, se están realizando según lo estipulado en las políticas y definición de procedimientos internos, y en concordancia con la ley Nº 19.886 correspondiente a la Ley de compras publicas.

Actividades de control

I) La Sección de Abastecimiento planifica y ejecuta un plan anual de compras según la reglamentación del HCHM.

La Sección de Abastecimiento cumple con la planificación y ejecución de un plan anual de compras, el cual es elaborado durante los últimos 2 meses del año donde se consideran los consumos históricos y los consumos del periodo en curso.

Este programa se ejecuta posteriormente mes a mes, lo que permite manejar tiempos razonables que evitan el desabastecimiento de alguna unidad de productos especifica. De igual manera cada producto cuenta con un stock critico el cual es controlado por el Sistema ANITA.

II) Se controla la recepción de los insumos y se almacenan según las disposiciones del HCHM.

La Sección de Abastecimiento cumple con la recepción de los insumos según la reglamentación y políticas establecidas, con lo que se maneja de manera transparente la relación con proveedores, en caso de producirse diferencias en las cantidades adquiridas y recepcionadas, el Sistema ANITA permite realizar el seguimiento al proceso de licitación y contrastar con la documentación adjuntada en el pedido por parte de los proveedores, en caso que no se logre esclarecer, se aplica el procedimiento creado para la devolución de los insumos.

III) Se monitorea la distribución de insumos sea acorde a las solicitudes efectuadas por las diferentes unidades clínicas del HCHM.

El proceso de distribución realizado por la Sección de Abastecimiento y es monitoreado de acuerdo a lo establecido en las políticas que maneja el HCHM, las cuales establecen diversas instancias de control, que se controlan mediante formularios los que permiten transferir la responsabilidad y el dominio sobre los despachos.

3.2.3. Planeación de la Continuidad del Negocio

3.2.3.1. Objetivos de control: En caso de desastre, los procesos del HCHM esenciales y los Sistemas de Información pueden ser recuperados oportunamente.

Actividades de Control.

I) La dirección ha elaborado y aprobado un plan general de continuidad con base en una evaluación del impacto.

La dirección no ha establecido un plan general para dar continuidad a los Sistemas de Información. Sin embargo el personal que es encargado de la manutención y respaldo de los sistemas ha establecidos reglas no escritas para el manejo de contingencias. Si existen contratos que aseguran el Hardware donde están contenidos los Sistemas de Información, los cuales ante un posible daño las piezas serán reemplazadas en un lapso de 24 horas. Mientras que para el respaldo de la información se realizan respaldo donde todos los días se realiza un respaldo denominado a nivel 0 el cual respalda todas los archivos en cinta, así como también todos los días jueves se realizan respaldo completo de cuentas de usuario, datos y sistemas, información que es traspasada a disco posteriormente.

Ante una falla que inhabilite los Sistemas de Información, que soportan los procesos manejados por la Sección de Abastecimiento se procederá como se detalla a continuación:

Proceso de adquisiciones: considerando que la Sección de Abastecimiento realiza las compras de forma mensual, el hospital maneja ciertos stocks críticos que permiten retrasar el registro de las licitaciones en los sistemas de control interno como es el caso del Sistema ANITA, hasta que este sea restablecido.

Proceso de recepción: El proceso de recepción de productos puede ser manejado en forma manual mediante cotejo de las guías de despacho y las ordenes de compra, al existir alguna diferencia esta es informada al proveedor y dependiendo del tipo de inconsistencia se puede proceder a aceptar el envió o cancelarlo para realizar una nueva adquisición.

Proceso de distribución: al igual que los otros procesos anteriores este puede ser realizado en forma manual, esta información es posteriormente ingresada a los sistemas una vez que estos se encuentran restablecidos.

3.2.4. Capacitación a los usuarios

3.2.4.1. Objetivos de control: Los usuarios reciben una capacitación apropiada y un apoyo continuo.

Actividades de control

I) La dirección monitorea el origen y frecuencia de las solicitudes de apoyo para determinar si se debe mejorar la capacitación de los usuarios, los recursos de apoyo y/o la documentación. Además de ejecutar procesos de captura de requerimientos que abarquen el área en su totalidad.

La captura de requerimientos no involucra a los usuarios finales del sistema, lo que produce que en ciertos casos no se implementen ciertos tipos de informes que son necesarios y que deben ser elaborados en forma manual.

En el HCHM no se realizan capacitaciones, que permitan a los usuarios familiarizarse con los sistemas antes de su implantación definitiva, lo que ha provocado que sistemas implantados no sean utilizados, como lo ocurrido con el sistema que apoya los pedidos y la distribución de los insumos, mediante el cual solo se realiza el 2% de los solicitudes de insumos mientras el 98% restante se realiza mediante formulario manual.

Por otra parte no existe un registro que permita monitorear el origen y frecuencia de las fallas que generan solicitudes de apoyo, que presenta tanto la Sección de Abastecimiento, como en las diferentes áreas que componen el HCHM. En esta materia el HCHM asumió una serie de compromisos con el MINSAL.

Dentro de los compromisos asumidos están:

a) Se deberá mantener un registro de los equipos y usuarios que presentan aparición de virus informático o Malware. Para ello se deberá realizar revisión 1 vez al mes del historial de los Software de contención.

Para el cual se estableció un plazo limite de implementación de Junio del 2009, el cual no se encuentra implementado.

Estado Actual: No se dispone del registro de aparición de virus, Malware implementado a pesar que los antivirus en cada equipo mantienen un registro de aparición. De igual manera no se posee un registro que permita monitorear los otros tipos de falla que se presentan en la Sección de Abastecimiento como en otras áreas.

b) Se deberá disponer de un manual de usuario para la prevención de Software malicioso y para el uso del Software de contención y eliminación. Manual elaborado, difundido y disponible en la intranet

Para el cual se estableció un plazo limite de implementación de Marzo del 2009, el cual no se encuentra implementado

Estado Actual: No se ha elaborado el manual para la prevención de infección por Software malicioso y educación en el uso del Software de eliminación y contención.

II) La documentación actual del usuario y documentación del sistema para los Sistemas de Información, se encuentra fácilmente disponible para el personal que lo requiera.

La documentación de apoyo se encuentra disponible tanto para el Sistema ANITA, mientras que el manual de apoyo correspondiente al Sistema HERMINDA se encuentra disponible pero se encuentra inconcluso, y no está en los planes de la Oficina de Ingeniería de Sistemas finalizarlo. La documentación del Sistema ANITA se encuentra desactualizada debido a que se han efectuado diversas modificaciones que las cuales no se han documentado.

El análisis y evaluación de riesgos indica que este ítem tiene un riesgo **importante,** por lo cual se deben poner los recursos suficientes para llevar a cabo procesos de capacitaciones. Se solicita prestar especial atención a este ítem por lo complejo que resulta mantener el personal sin las herramientas y conocimientos necesarios para su óptimo desempeño.

En relación a las actualizaciones de los sistemas se detecto la existencia de un riesgo **importante**, debido a que existen nuevos requerimientos de los usuarios que no han sido considerados, comprometiendo un servicio eficiente.

3.2.5. Administración de datos

3.2.5.1. Objetivos de control: Respaldo y Restauración.

Actividades de control

I) La dirección y los usuarios planean y programan el respaldo y retención de información, así como la cancelación y liberación de los medios cuando ya no se requiere la retención

El hospital específicamente el Área de Soporte de Comunicaciones esta encargado para respaldar y dar soporte al Sistema ANITA, estos respaldos son realizados en cintas magnéticas, estas cintas son utilizadas en forma alternada manteniendo la información de 2 días. Para este procedimiento no existe un reglamento formal escrito. Mientras que para el Sistema HERMINDA se utiliza un servidor espejado.

II) Los respaldos se archivan fuera del sitio donde se generaron para minimizar el riesgo de que se pierdan la información.

No existe una reglamentación para el manejo de los respaldos. De este modo los respaldos del Sistema ANITA son conservados en el mismo lugar donde se generan los respaldos, manteniendo todas las copias en un mismo lugar. Mientras que el Sistema HERMINDA mantiene el servidor espejado en la misma sala de cómputo que los servidores del Sistema ANITA, por lo que no se cumple el objetivo de mantener copias de la información en lugares diferentes ante un posible siniestro.

III) Todos los medios (cintas, manuales, documentación, etc.) son almacenados en un lugar seguro de ambiente controlado.

No existe una reglamentación que estipule claramente la manipulación de las cintas y documentos de los Sistemas de Información, por lo que no se ha designado un lugar aislado que permita garantizar la integridad de dichos medios.

IV) Los dispositivos removibles son rotulados para permitir su debida identificación.

Al no existir una reglamentación formal y escrita, que estipule el manejo de los respaldos y dado que solo se cuenta con 2 dispositivos de cintas, para la realización de las tareas de respaldo, estas no se rotulan como estipulan las buenas practicas de seguridad de información.

V) En caso de un desastre, el Sistema de Información pueden recuperarse en un tiempo razonable.

Al no existir una reglamentación que estipule los procedimientos a seguir en caso de que ocurra algún desastre donde se pierda la información, se desconoce cual será el tiempo de respuesta en caso, que los sistemas se vean expuestos a algún siniestro mayor. Solo se cuenta con contratos que establecen la recuperación del Hardware que soporta el sistema ANITA.

VI) Restablecimiento de la información bajo un ambiente controlado.

Al no existir una reglamentación que estipule los procedimientos a seguir en caso contingencias mayores, no se realizan pruebas de restablecimiento de datos a partir de las cintas o del disco duro que se utilizan en el Área de Soporte de Comunicaciones para la realización de los respaldos.

El análisis y evaluación de riesgos indica que este ítem tiene un riesgo **importante,** debido a que no existen políticas formales y procedimientos adecuados para el resguardo de la información.

3.3. Análisis y Evaluación de Riesgos

3.3.1 Amenazas Detectadas

Realizado el proceso de análisis de la información obtenida, proveniente de; documentación, inspección de las dependencias de la organización, verificación de los procesos llevados a cabo. Con toda la información recopilada se ha detectado una serie de amenaza que pueden atentar contra los activos de la institución, como son la información, Sistemas de Información, equipamiento y personas.

La **tabla 2** muestra las amenazas detectadas y su factor de criticidad determinado.

Tipo de Amenaza	Factor Criticidad
Accesos no Autorizados	Alto
Errores de Usuarios	Medio
Continuidad del Servicio	Alto
Virus, Malware	Alto
Mantenimiento de Equipos	Medio
Siniestros	Bajo
Desastres Naturales	Bajo
Planes de Contingencia	Medio
Robos, Mermas	Medio
Integridad de Datos	Alto
Seguros	Medio
Revelación de Información	Alto
Ataques Externos	Bajo
Software de Terceros	Medio
Capacitación	Medio
Actualización de los Sistemas de Información	Medio
Respaldos y Restauración	Alto
Organización y Distribución de Responsabilidades.	Medio

Tabla 2: Amenazas Detectadas

La evaluación de los riesgos detectados que se muestran en la Tabla 2 se detalla en el anexo VI, y las conclusiones alcanzadas son parte fundamental de la evidencia que sustenta la opinión de la Auditoría.

CAPÍTULO IV - INFORME DE AUDITORÍA INFORMÁTICA

4.1. Introducción.

En este capítulo se presenta el informe de Auditoría Informática, el que contiene la opinión emitida por Equipo Auditor, la evidencia que lo sustenta y las sugerencias propuestas.

4.2. Carta de Auditoría

Chillán, 23 de diciembre de 2009

Sr. Luís San Martín Hernández
Subdirector Administrativo
Hospital Clínico Herminda Martín

Presente

De nuestra consideración:
En la Auditoría Informática a la Sección de Abastecimiento del Hospital Clínico Herminda Martín de Chillán, llevada a cabo entre los meses de Agosto a Diciembre del presente año, se sometió a evaluación a los Sistemas de Información que gobiernan las actividades de la sección auditada. El objetivo era verificar la utilización que los usuarios hacen de ellos y la contribución de los mismos a la consecución de los objetivos que la sección persigue. Además de evaluar los procedimientos claves de la sección y su correcta ejecución, las medidas de seguridad física y lógica que resguardan los activos de la institución.

Durante la ejecución del proceso se abordaron temáticas aún más amplias que las propias de la Sección de Abastecimiento, entre los cuales podemos mencionar los procedimientos, controles y seguridad implantada en áreas que brindan soporte a la sección objeto de Auditoría, como son la Oficina de Ingeniería de Sistemas y el Área Soporte de Comunicaciones. Se consideró relevante la evaluación de las áreas mencionadas puesto que estas juegan un papel importante en la entrega de un servicio eficiente por parte de la Sección de Abastecimiento.

Le indicamos que el objetivo fundamental del proceso realizado es la formulación de una opinión del estado actual de la Sección de Abastecimiento, basada en la evaluación de la

información recabada, y sustentada en los hallazgos detectados, que serán detallados para un mayor entendimiento y contribución a la toma de decisiones, por parte de la Dirección.

El Equipo Auditor reafirma que en todo momento se intentó mantener su compromiso de transparencia e imparcialidad en el proceso y juicio emitido, mantuvimos una actitud profesional e independiente en cada una de las actividades realizadas, por lo cual validamos ante nuestro criterio la opinión emitida.
La opinión del Equipo Auditor es con salvedades. El sustento de la opinión brindada se encuentra resumida en el punto 7 del Informe de Auditoría, denominado Conclusiones y es avalado por la evidencia recopilada y la evaluación de la misma, bajo el criterio objetivo e independiente del Equipo Auditor.

Los hallazgos detectados se encuentran detallados en el punto 8 del Informe de Auditoría, denominado Resultados, en el se encontrará un resumen en se indican las consideraciones del Equipo Auditor hacia los procedimientos, controles y prácticas presentes en la Sección de Abastecimiento y las áreas que le brindan servicios, como lo son la Oficina de Ingeniería de Sistemas y el Área de Soporte de Comunicaciones. Además se plantea una propuesta de solución para cada hallazgo detectado, las cuales esperamos usted pueda considerar a tratar.

Este informe es únicamente para conocimiento y uso de la Subdirección Administrativa del Hospital Clínico Herminda Martín, y queda a su criterio la difusión del mismo.

Agradecemos la colaboración dispensada durante el desarrollo del proceso de Auditoría Informática por el personal del Hospital Clínico Herminda Martín. Destacamos la actitud proactiva y colaborativa de los funcionarios, que atendieron mayoritariamente a las peticiones solicitadas.

Sin otro asunto que abordar, quedamos a su disposición para aclarar o ampliar cualquier materia contenida en el presente informe.

Saludamos atentamente a usted,

_____	_____
Julio Contreras Jeldres	Cristian Chandia Poblete

4.3. Estructura del Informe

La estructura del Informe de Auditoría Informática utilizada es la descrita en el Capítulo IV, del libro, Auditoría Informática Un Enfoque Práctico (2ª Edición Ampliada y Revisada, ALFOMEGA, 2001), y aborda los siguientes puntos:

4.3.1. Identificación del Informe
4.3.2. Identificación del Cliente
4.3.3. Identificación de la Entidad Auditada
4.3.4. Objetivos de la Auditaría Informática
4.3.5. Normativa Aplicada y Excepciones
4.3.6. Alcance de la Auditoría
4.3.7. Conclusiones
    4.3.7.1. Opinión de la Auditoría
    4.3.7.2. Resumen de la Opinión
4.3.8. Resultados
4.3.9. Informes Previos
4.3.10. Fecha del Informe
4.3.11. Identificación y Firma del Auditoría
4.3.12. Distribución del Informe.

4.3.1. Identificación del Informe

Informe de Auditoría Informática a la Sección de Abastecimiento del Hospital Clínico Herminda Martín de la Ciudad de Chillán.

4.3.2. Identificación del Cliente

El proceso de Auditoría ha sido encargado por el Señor Luís San Martín, Subdirector Administrativo del Hospital Clínico Herminda Martín de la Ciudad de Chillán.

4.3.3. Identificación de la Entidad Auditada

La entidad sometida al proceso de Auditoría Informática es la Sección de Abastecimiento y Bodega, dependiente del Subdepartamento de Abastecimiento y Finanzas, el cual depende directamente de la Subdirección Administrativa del Hospital Clínico Herminda Martín.

4.3.4. Objetivos de la Auditaría Informática

- Realizar una Auditoría informática externa de carácter independiente y profesional.
- Verificar la calidad de los Sistemas de Información, uso y procedimientos que gobiernan la Sección de Abastecimiento del Hospital Clínico Herminda Martín de la ciudad de Chillán.
- Verificar el estado de seguridad en la sección y la de aquellos que le brindan servicios.
- Verificar la existencia de políticas que normen los procedimientos, la seguridad y los planes de contingencia.
- Verificar la existencia de la documentación adecuada.

4.3.5. Normativa Aplicada y Excepciones

- Se verificó el cumplimiento de la Ley Nº 19.886, Ley de Compras y Reglamento, que rige las adquisiciones de todas las instituciones públicas.

- Se verificó el cumplimento de los compromisos de seguridad adquiridos con el Ministerio de Salud, comprendidos en el documento de Políticas de Seguridad para el sector salud, de Junio de 2008.
- Se verificó el cumplimiento de la normativa interna que rige los procedimientos y responsabilidades de la Sección de Abastecimiento. Se utilizó el documento denominado Manual de Organización, Sección de Abastecimiento Hospital Clínico Herminda Martín de Chillán.
- Los procedimientos no establecidos se evaluaron con las buenas prácticas sugeridas en el COBIT 4.0. La utilización del COBIT se limita al dominio de Entrega y Soporte (DS).

4.3.6. Alcance de la Auditoría

4.3.6.1. Alcance

La Auditoría se realizó a la Sección de Abastecimiento del Hospital Clínico Herminda Martín de Chillán. Se analizaron los procesos relevantes como lo son; los procesos de compra, recepción y almacenamiento, en búsqueda de deficiencias.

La Auditoría considera el análisis de los Sistemas; ANITA que gobierna las actividades de la Sección de Abastecimiento, Sistema de Costos HERMINDA, de forma general. Se contempla además la revisión de la documentación perteneciente a los sistemas.

Además se contemplará el análisis y evaluación de los procedimientos y políticas de seguridad, física y lógica de la sección, y de la Oficina de Ingeniería de Sistemas y el Área de Soporte de Comunicaciones,

Esta Auditoría no sometió a evaluación al Sistema Gubernamental Mercado Público, por tratarse de un sistema cuya administración no recae sobre la institución Auditada, como tampoco al Sistema PYXIS puesto que se encuentra en proceso de puesta en marcha.

4.3.6.2. Extensión

El proceso de Auditoría realizado tuvo una extensión de 4 meses, a partir del mes de agosto al mes de noviembre del año 2009.

4.3.6.3. Limitaciones al Alcance

Se indica que no existieron mayores limitaciones al alcance, se mostró un trabajo colaborativo por parte del personal, entregando mayoritariamente la información solicitada, se nos hizo saber que la información que no se entregaba era por que no existía, entiéndase manuales de seguridad, manuales de uso, políticas, etc.

Se ha facilitado siempre el ingreso a las dependencias y se concretaron mayoritariamente las reuniones acordadas, las reuniones no concretadas fueron excusadas por falta de disponibilidad.

No se pudo comprobar empíricamente el proceso de recepción de productos debido a que esta se realizaba fuera de horarios de oficina.

Sólo se pudo comprobar empíricamente el procedimiento de contingencia para la distribución de productos, los demás procedimientos no presentaron instancias de control para los planes de contingencia.

Por motivos de seguridad de la institución no se pudo manipular los Sistemas de Información y bases de datos, pudiendo verificar su funcionamiento mediante el uso por parte del personal del Hospital.

4.3.7. Conclusiones

4.3.7.1. Opinión de la Auditoría

El Equipo Auditor, conformado por Julio César Contreras Jeldres y Cristian Alejandro Chandía Poblete, manifiesta una opinión; ***Con salvedades.***

4.3.7.2. Resumen de la Opinión

La opinión es justificada por los siguientes argumentos:

- La Sección de Abastecimiento cumple con la reglamentación, políticas ministeriales y leyes gubernamentales.

- Los procedimientos fundamentales como, adquisición, distribución, facturación, y recepción, se encuentran debidamente documentados y se verifica su correcta ejecución. Dichos procedimientos se encuentran en constante revisión en busca de mejoras.
- Los procedimientos se apoyan mayoritariamente por los Sistemas de Información dispuestos por la institución, beneficiando a la transparencia de los procesos.
- Los funcionarios cumplen con las labores estipuladas en el manual de la organización.
- Se garantiza la continuidad de los procedimientos fundamentales en caso de contingencia. Debido a que se encuentran capacitados para realizar las funciones sin contar con los Sistemas de Información.

Pero a pesar de lo mencionado como favorable en los puntos anteriores, existen salvedades como:

- No se cuenta con políticas de seguridad definidas formalmente, tanto para la Sección de Abastecimiento como para el Área de Soporte de Comunicaciones.
- Los Sistemas de Información utilizados no cumplen a cabalidad con los requerimientos de los usuarios y del servicio.
- No se realizan capacitaciones formales para los usuarios finales, los cuales además no participan en la captura de requerimientos, tanto para los nuevos sistemas como para las actualizaciones.
- Se verifica que la documentación no se encuentra actualizada.
- El manual de uso del Sistema HERMINDA no se encuentra debidamente detallado.
- No existen políticas formales para el respaldo y restauración de la información.
- El registro de ingresos de los productos se realiza de forma manual, lo que aletarga el procedimiento e induce al error.

- En el procedimiento de almacenaje no se registran todos los datos necesarios para un adecuado control de stock.
- El Sistema ANITA no permite el registro del plan anual de compras, el cual se elabora en planillas de cálculo, las cuales se deben ingresar mensualmente de forma manual al sistema. Esto no permite diferenciar entre una compra planificada y extraordinaria, lo que no contribuye a buena gestión de los recursos de la institución.
- No existe comunicación entre el Sistema ANITA y el Sistema Gubernamental Mercado Público, lo que implica que cada licitación deba ser ingresada o transcrita en ambos sistemas, para cumplir con las normativas legales vigentes.
- Las bases de datos de los Sistemas de Información no se encuentran encriptadas, comprometiendo la confidencialidad y la seguridad en general de la información.
- Existe un riesgo fundado en que la información reflejada por el Sistema ANITA no concuerde con la información real.
- No existe un control de acceso a las instalaciones definido y difundido tanto para la Sección de Abastecimiento como para el Área de Soporte de Comunicaciones. Sólo se mantienen buenas prácticas de seguridad

4.3.8. Resultados

4.3.8.1. Seguridad de la información.

Seguridad Lógica.

a) Al efectuar revisión se detectó una debilidad en la organización de los departamentos encargados del manejo de los Sistemas de Información, utilizados por la Sección de Abastecimiento, puesto que no existe una unidad que dictamine que reglas se deben seguir dentro de la organización en materia de seguridad de la información, con lo que cada unidad de las involucradas trabaja de forma separada, una de las principales razones es por la estructura que tiene el hospital

clínico al cual pertenece la Oficina de Ingeniería de Sistemas y la Sección de Abastecimiento, mientras que el Área de Soporte de Comunicaciones depende del departamento de recursos físicos del Servicio de Salud Ñuble. Por otra parte existen compromisos adquiridos en materia seguridad, de cuales no ha existido la instancia que permita el control de su cumplimiento.

Recomendamos que para la elaboración del listado de sitios Web prohibidos se conforme un comité con miembros de las diferentes áreas involucradas, tanto directivos, personal del Área de Soporte de Comunicaciones, personal de la Oficina de Ingeniería de Sistemas y personal de la Sección de Abastecimiento, generando una instancia que permita unificar ideas y recursos en el tema de seguridad de la información.

b) Nuestra revisión detectó que no existe un plan que permita mantener un control sobre los errores de acceso en los sistemas, el Sistema ANITA tiene implementado el bloqueo de cuenta al ingresar en forma errónea, mientras que el Sistema HERMINDA no tiene implementada esta medida, lo que lo expone a algún ataque de fuerza bruta.

Los errores generados en la operación del Sistema ANITA se refieren principalmente al ingreso erróneo de las licitaciones, esto queda registrado en el sistema mediante un estado adicional 6, sin embargo estos errores solo son monitoreados en caso de que se presenten diferencias en las compras de insumos, de forma correctiva y no de forma preventiva.

Recomendamos la implementación del bloqueo de cuentas de usuario en caso que se generen ingresos erróneos reiterados, ya que actualmente no se tiene considerado el riesgo que la información

pueda ser robada y sea utilizada como información privilegiada por proveedores. Por otra parte se sugiere el monitoreo de los errores que se generan en el Sistema ANITA y tomar las medidas correctivas necesarias.

c) Al efectuar la revisión se detecto que no existen políticas formales que indiquen los cambios de claves, ni tampoco que establezcan la composición de estas. Actualmente realizar este cambio es posible mediante una solicitud al personal del Área de Soporte de Comunicaciones para el Sistema ANITA y al personal de la Oficina de Ingeniería de Sistemas para el Sistema HERMINDA. Mientras que los privilegios de los sistemas no son modificados frecuentemente a pesar de existir la necesidad que esto se realice.

d) Se detectó que las cuentas de usuario son de carácter único, sin embargo la asignación de privilegios de cada cuenta del Sistema ANITA no esta actualizada a las necesidades del personal de la Sección de Abastecimiento.

Recomendamos la elaboración de políticas formales y escritas que definan los procedimientos para los cambios de claves, dar de alta y baja un determinado perfil de usuario. De esta forma garantizar que las cuentas sean personales y no sean utilizadas por más de un usuario.

Se recomienda un proceso de Auditoría de las cuentas de usuario para verificar cuales se encuentran activas, con la finalidad de eliminar todas aquellas cuentas de personal que ya no pertenece a la institución o han sido asignados a otro cargo. También existen compromisos de seguridad que no se encuentran implementados en su totalidad.

Además como parte fundamental de la seguridad lógica se sugiere la codificación de la base datos, al menos en los campos principales como son claves de los usuarios, información confidencial de pacientes, licitaciones, entre otros

Seguridad Física.

a) Se comprobó que el acceso a sala de servidores se encuentra restringido a personal que no pertenezca al Área de Soporte de Comunicaciones y de la Oficina de Ingeniería de Sistemas, sin embargo no se encuentran implementados en su totalidad los compromisos asumidos que hacen alusión a la definición del personal responsable de la seguridad de acceso a la sala de servidores.

Recomendamos establecer las instancias que reúnan a directivos, personal del hospital y personal encargado de la seguridad de la información del Servicio de Salud Ñuble, para definir responsabilidades y compromisos de cada una de las partes involucradas.

Seguridad física, lógica y riesgos asociados.

a) Se comprobó que no se ha realizado un análisis y evaluación de riesgos asociados a la Sección de Abastecimiento, ni a las áreas que proporcionan soporte, como son el Área de Soporte de Comunicaciones y la Oficina de Ingeniería de Sistemas.

Recomendamos llevar a cabo el análisis de riesgo identificando las amenazas que pueden afectar a los activos de la institución y el real impacto de su ocurrencia. Esto puede contribuir a una mejor distribución de los recursos. Se sugiere además que este análisis sea

realizado no solo por la Sección de Abastecimiento, sino que también involucre a otras unidades críticas del centro hospitalario.

Protección frente a Software malicioso.

a) Se comprobó que la totalidad de los equipos computacionales cuentan con Software de antivirus licenciado, y como medida complementaria se limitan los privilegios para los Sistemas Operativos, no permitiendo la instalación de programas que puedan contener malware, para poder llevar a cabo la instalación se requiere la autorización especial por parte del personal del Área de Soporte de Comunicaciones.

   Recomendamos implementar la limitación de los perfiles en la totalidad de los equipos del hospital, tal como se asumió en el compromiso contraído con el ministerio de salud.

b) Se comprobó que la información no es cargada directamente a los Sistemas la Información proporcionada al Sistema ANITA es ingresada en forma manual por cada ejecutivo del área. Mientras que la información del Sistema HERMINDA es obtenida directamente desde las bases de datos de los diferentes Sistemas de Información y ambas se encuentran libres de virus.

c) Se detectó que las actualizaciones de las firmas de virus, son puestas a disposición del personal en un servidor propio, sin embargo esto no garantiza que los usuarios actualicen los equipos.

   Recomendamos configurar los equipos para que la actualización sea realizada en forma automática por el Software de antivirus.

Seguridad Ambiental.

a) Se detectó que la dirección no es la encargada de monitorear las actividades de control referentes a la seguridad ambiental, estas recaen en el personal de la Sección de Abastecimiento, el Área de Soporte de Comunicaciones y la Oficina de Ingeniería de Sistemas. Estas a su vez no tienen establecidos las responsabilidades, medidas y controles de manera formal.

Recomendamos elaborar un comité que permita establecer las responsabilidades, medidas y controles de manera formal, asesorándose por personal experto en materia de seguridad.

b) Se detectó que solamente el servidor que contiene el Sistema ANITA se encuentra resguardado con UPS, el resto de los equipos no se encuentra protegido. Además el compromiso de resguardar con UPS todos los equipos denominados como críticos, se encuentra implementado en un 80%.

Recomendamos la implementación de UPS para los demás servidores, como también para la totalidad de los equipos definidos como críticos, para evitar posibles daños tanto en Hardware y Software.

Relación con proveedores externos y clientes.

a) Se comprobó que la Sección de Abastecimiento realiza el proceso de planificación de compras y la ejecución de este, de a cuerdo a la reglamentación existente. Sin embargo se detectó la replicación del proceso de registro, el que se detallará a continuación.

- Se elabora un programa anual de compras en tablas Excel, las que se van ejecutando mes a mes.

- Se registra el proceso de licitación correspondiente a una compra en el Sistema ANITA, este procedimiento de digitación se realiza en forma manual.
- La información registrada en ANITA es transcrita al portal mercado público para su licitación.

Recomendamos la unificación de la etapa 1 y 2 de este proceso, desarrollando un módulo, que permita cargar datos desde las tablas donde se elabora el programa anual de compras en primera instancia. Además se sugiere analizar la factibilidad de carga masiva de licitaciones el portal www.mercadopublico.cl.

b) Se comprobó que la Sección de Abastecimiento realiza el proceso de recepción de compras y almacenamiento de acuerdo a la reglamentación existente para este proceso. Sin embargo en el procedimiento de almacenaje de los insumos, no se cuenta con códigos que identifiquen los lotes de productos en forma independiente, además de no tener definidos en su totalidad la conversión unitaria de los productos lo que genera diferencias entre lo adquirido y lo almacenado.

Recomendamos implementar el sistema de código de barras que permita el ingreso masivo de productos aumentando su eficiencia y seguridad. Además un nuevo atributo o dato que permita diferenciar los productos que son iguales pero que fueron adquiridos en fechas diferentes, con esto manejando de mejor manera el control de stock y los vencimientos de los productos.

c) Se comprobó que la Sección de Abastecimiento realiza el proceso de distribución de productos en conformidad con la reglamentación existente para este proceso. Sin embargo el procedimiento podría ser

mas eficiente dado la baja utilización del Sistema de Información destinado a este proceso que solo alcanza el 2%.

Recomendamos realizar capacitaciones a las diferentes unidades de tal manera que se pueda masificar el uso del sistema destinado a la distribución.

Recuperación de los Sistemas.

a) Se comprobó que la dirección no ha establecido planes para la continuidad de los sistemas, sin embargo las diferentes planes de contingencia para el manejo de la información cuando los Sistemas de Información se encuentran inhabilitados, de esta forma la Sección de Abastecimiento puede mantenerse operativa realizando los procesos de forma manual, luego cuando el Sistema ANITA se encuentra nuevamente operativo se procede a registrar la información de las transacciones.

   Por otra parte el Área de Soporte de Comunicaciones, es la encargada del restablecimiento de los sistemas para lo cual cuenta con diferentes medidas establecidas, las que no se encuentran documentadas.

   Recomendamos elaborar un comité que se encargue de revisar y redactar las políticas existentes de manera formal, para el restablecimiento de los Sistemas de Información y planes de contingencia para la Sección de Abastecimiento.

Capacitación de los usuarios.

a) Se detecto que tanto Dirección, como el Área de Soporte de Comunicaciones y la Oficina de Ingeniería de Sistemas, no realizan el monitoreo de los errores presentados esto por que no existe un registro de los errores que permita hacer el seguimiento.

   Además se comprobó que la Oficina de Ingeniería de Sistemas no realiza capacitaciones a los usuarios finales de los sistemas que se

implantan, esto facilitado en gran medida por la no existencia de políticas que exijan esto.

Se detecto que la captura de requerimientos solo considera la opinión de los jefes de las áreas involucradas no considerando las opiniones de los usuarios finales, lo que ocasiona produce que la captura de requerimientos no sea optima.

Recomendamos elaborar nuevamente el manual usuario del Sistema HERMINDA, mantener un registro de los errores a los cuales da soporte para verificar el origen y causa de los errores, y además elaborar un medio de difusión para el sistema de pedidos hospitalario que se encuentra operativo con solo un 2% de las operaciones realizadas a través de este medio. Se recomienda además incluir en el proceso de desarrollo o modificación de un sistema una muestra significativa de usuarios finales de los sistemas para cubrir la mayor cantidad de necesidades que sean posibles

También existen compromisos asumidos que no se encuentran implementados.

b) Se comprobó que tanto los manuales de usuario de los Sistemas ANITA y HERMINDA se encuentran disponibles para la Sección de Abastecimiento, el manual usuario de pedidos hospitalarios no se encuentra disponible. Además se comprobó que las modificaciones realizadas al Sistema ANITA no han sido debidamente documentadas.

Recomendamos elaborar un manual de usuario para el sistema de pedidos hospitalarios que sirva además como método de difusión, y además la elaboración de un nuevo manual para el Sistema HERMINDA. Para el Sistema ANITA se recomienda actualizar la documentación existente del sistema.

Respaldo y restauración.

a) Se comprobó la existencia de políticas y el cumplimiento de estas para la ejecución del proceso de respaldo del Sistema ANITA, estas políticas no se encuentran formalmente escritas pero son de conocimiento del personal del Área de Soporte de Comunicaciones.
Recomendamos la elaboración de un manual que contenga políticas formales para llevar a cabo el proceso de respaldo.

b) Se comprobó que los respaldos son almacenados en el mismo lugar donde son generados, con lo cual no cumple una parte de los objetivos de los respaldos que es aislar las copias de seguridad existentes, para que en caso de ocurrir un siniestro la información pueda ser recuperada.

c) Se comprobó que los respaldos son no son almacenados en lugares seguros, y son mantenidos en el mismo lugar donde son generados.
Recomendamos incluir en la elaboración del manual de políticas de respaldo, un procedimiento que permita aislar las copias de seguridad de la información y mantenerlas en un lugar seguro.

d) Se comprobó la existencia de 2 cintas las se encuentran rotuladas permitiendo así la identificación de ambas, pero al no existir una política formal que establezca que cinta es la mas actualizada, no se cumple el objetivo en su totalidad.
Recomendamos incluir en la elaboración de las políticas un planificación de respaldo que permita especificar cual de ambas cintas es la que posee la información mas actualizada. De igual manera se sugiere establecer un periodo de vida útil según el uso que tienen estos medios, para facilitar su recambio.

e) Se comprobó la existencia de seguros en caso de daños de Hardware, que asegura el restablecimiento los dispositivos que puedan presentar fallas, en el servidor que contiene el Sistema ANITA, además se comprobó que no existen seguros para el restablecimiento de Software y datos contenidos en dicho servidor.

   Recomendamos incluir en la elaboración de las políticas que establezca que procedimiento se deberá realizar en caso que los dispositivos de cintas no puedan restablecer los sistemas y las bases de datos. Además se recomienda ampliar la cobertura del seguro existente para el restablecimiento de los sistemas y bases de datos contenidas en este servidor dado corresponde al servidor central, de esta forma evitar posibles pérdidas de información irreparables como ha ocurrido anteriormente.

f) Se detectó la ausencia de pruebas de comprobación de los respaldos y pruebas de restablecimiento de la información.

   Recomendamos incluir en la elaboración de las políticas que se establezca un procedimiento que asegure que los respaldos han sido completados de manera exitosa.

4.3.9. Informes Previos

No se utilizó información proveniente de informes de auditorías previamente realizadas en la institución.

4.3.10. Fecha del Informe

Fecha inicial del Trabajo: Martes 18 de Agosto de 2009.

Fecha Final del Trabajo en Terreno: Viernes 25 de Noviembre de 2009.

Fecha Final del Proceso de Auditoría: Martes 22 de diciembre de 2009

4.3.11. Identificación y Firma del Auditoría

El Equipo Auditor que llevo a cabo el proceso de Auditoría Informática en la Sección de Abastecimiento del Hospital Clínico Herminda Martín de Chillán, esta conformado por:

Julio Contreras Jeldres, Alumno de la Carrera de Contador Público y Auditor, de la Universidad del Bío-Bío, Sede Chillán.
Cristian Chandía Poblete, Alumno de la Carrera de Ingeniería de Ejecución en Computación e Informática, de la Universidad del Bío-Bío, Sede Chillán.

Los cuales certifican que el proceso realizado se hizo intentando mantener siempre la independencia y el profesionalismo.

_____	_____
Julio Contreras Jeldres	Cristian Chandía Poblete

4.3.12. Distribución del Informe

Se hará efectiva la entrega de una copia del Informe de Auditoría a las siguientes personas;

- Luís San Martín, Subdirector Administrativo del Hospital Clínico Herminda Martín de Chillán.
- Raúl Vielma, Jefe de la Sección de Abastecimiento del Hospital Clínico Herminda Martín de Chillán.

CONCLUSIONES

El proyecto desarrollado ha derivado en un estudio más amplio de lo estipulado en un comienzo. El carácter práctico del estudio realizado a permitido al Equipo Auditor comprobar las reales dimensiones y temáticas relevantes para la Auditoría Informática. Dicha Auditoría surgió como una necesidad de la Dirección de contar con información actualizada del uso de las tecnologías y Sistemas de Información y la contribución de estos a labor realizada por la Sección de Abastecimiento del Hospital Clínico Herminda Martín de la Ciudad de Chillán y la consecución de sus objetivos.

El objetivo primordial que recae sobre el Equipo Auditor fue brindar a la Dirección de la Sección de Abastecimiento y Hospital, una evaluación detallada que entregase información que contribuya a la toma de decisiones relacionadas con la distribución de los recursos, resaltando los aspectos que requieren mayor control.

Es por esto que la Auditoría Informática amplió su horizonte a temáticas como la seguridad, procedimientos y la manipulación de los Sistemas de Información, materias que sumaron complejidad al proceso, debiendo complementar los conocimientos con documentación adicional que enriqueció el producto del trabajo realizado y aportó significativamente a la formación profesional del Equipo Auditor.

Abordando la temática de la conformación del Equipo Auditor, afirmamos con certeza que la conjunción de conocimientos que las diferentes formaciones profesionales adquiridas por ambos alumnos, contribuyó al cumplimiento general de los objetivos de la Auditoría, la cual de no contar aquella conformación hubiese limitado su alcance, y profundización, coartando las necesidades de la institución demandante.

El aporte real de los miembros del Equipo Auditor de forma general es;
Julio Contreras Jeldres, Alumnos de la Carrera de Contador Público y Auditor; aportar con la metodología empleada para el proceso de Auditoría y la planificación de ella,

desarrollo de herramientas de Auditoría, determinación de controles a efectuar, evaluación de riesgos.

Cristian Chandía Poblete, Alumno de la Carrera de Ingeniería de Ejecución en Computación e Informática; aportar con sus conocimientos en tecnologías de información, Sistemas de Información, seguridad informática, equipamiento computacional, desarrollo de aplicaciones.

Además del aporte individual debido a los conocimientos propios de nuestra formación, se logró dar cumplimiento óptimo a las actividades que conforman el proceso de Auditoría de forma conjunta y colaborativa. Siendo la evidencia recopilada, los controles efectuados, la evaluación de la información y la opinión formulada es producto del trabajo conciente y apegado lo más posible a lo profesional.

Cabe mencionar y en pos del profesionalismo de la labor realizada que no se logró profundizar en algunos temas que formaron parte de los objetivos planteados en un comienzo, quedando por abordar en detalle temas como tan importante como; bases de datos de los Sistemas de Información, debido a limitaciones de tiempo, operatividad de los planes de contingencia.

Por último destacamos el espíritu colaborativo del personal de la Sección auditada y de las áreas que le brindan servicio, que mantuvieron en todo momento una actitud proactiva ante nuestros requerimientos, entregando información relevante que formó parte del sustento de la Auditoría Informática. El documento desarrollado es parte del trabajo conjunto, responsable, profesional e independiente del Equipo Auditor, y nos permitió dar una opinión fundamentada del estado actual de la Sección de Abastecimiento, de los Sistemas de Información y procedimiento que la gobiernan. Esperamos que las recomendaciones elaboradas tengan una buena acogida por parte de la dirección, pues buscan el mejoramiento del servicio brindado.

BIBLIOGRAFIA

PIATTINI V., Mario y DEL PESO, EMILIO. Auditoría Informática Un Enfoque Práctico, 2ª Edición Ampliada y Revisada, ALFOMEGA, 2001. 660p.

DERRIEN, Yan. Técnicas de la Auditoría Informática, Barcelona, ALFAOMEGA, 1995. 229p.

PIATTINI V., Mario, DEL PESO, Emilio, DEL PESO, Mar. Auditoría de Tecnologías y Sistemas de Información. México. 2008. 732p.

IT Governance Institute. COBIT 4.0, IL, EE.UU, IT Governance Institute, 2005. 207p.

Ley Nº 19.886. CHILE. Ley de Compras Públicas y Reglamento. Gobierno de Chile, Santiago, Chile, 24 de octubre de 2004, 108p.

Políticas de Seguridad para el Sector Salud. Ministerio de Salud de Chile, Santiago, Chile, 19 de junio de 2008. 49p.

IBARRA A. Pablo E. Tesis Auditoría a la Seguridad y Control de la Información en ambiente Windows NT. Chillán, Chile. Universidad del Bío-Bío, Departamento de Auditora e Informática, 2000.

ANEXOS

ANEXO I – MARCOS DE REFERENCIA UTILIZADOS

1. COBIT

Da soporte al gobierno de tecnologías de información como se refleja en la figura 30, al brindar un marco de trabajo que garantiza que:

- Las Tecnologías de Información (TI) están alineada con el negocio.
- Las TI capacitan el negocio y maximiza los beneficios.
- Los recursos de TI se usen de manera responsable.
- Los riesgos de TI se administren apropiadamente.

Figura 29: Gobierno de TI

Alineación estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI, en definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de valor se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

Administración de recursos se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI, aplicaciones, información, infraestructura y

personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Administración de riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Medición del desempeño rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio.

1.1. Que es el COBIT

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de TI.

1.2. Marco de Trabajo de COBIT

La alta dirección de las organizaciones se dan cuenta de lo valioso que resulta ser la información y lo significativo que esta resulta para el éxito de las mismas. La dirección espera que el buen gobierno de TI le permita mantener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la organización es posible que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse

- Cuente con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las organizaciones exitosas entienden los riesgos que trae el negocio y aprovechan los beneficios de las TI.

El marco de trabajo proporcionado por COBIT es de utilidad para una variedad de interesados, tantos internos y externos, cada uno de los cuales tiene necesidades específicas. Algunos interesados pueden ser:

- Personal a cargo de la toma de decisiones de inversión.
- Personal que utilice los servicios de TI.
- Administradores de las organizaciones.
- Operadores de los servicios.
- Responsables de la seguridad y riesgos.

1.3. Criterios de Información de COBIT

COBIT indica que para dar cumplimiento con los objetivos de las organizaciones la información manejada debe adaptarse a ciertos criterios:

- **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 optimizando los recursos (más productivo y económico).
- **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.

- **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** significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

El ideal de cada organización es que pueda dar cumplimiento cabal a los criterios mencionados. Dependiendo de la función desempeñada por la organización se pondrán más énfasis en alguno de los criterios. En el caso del área sujeta a auditar, se busca cumplir en mayor medida con los criterios de eficiencia, confidencialidad, disponibilidad, cumplimiento.

1.4. Recursos de TI

Los recursos que el COBIT identifica son los siguientes:

- **Las aplicaciones** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **La información** son los datos en todas sus formas de entrada, procesados y generados por los Sistemas de Información, en cualquier forma en que son utilizados por el negocio.
- **La infraestructura** es la tecnología y las instalaciones (Hardware, Sistemas Operativos, Sistemas de Administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- **Las personas,** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

1.5. Procesos Orientados

COBIT define las actividades de Tecnologías de Información en 4 dominios, estos son:

- Planear y Organizar (PO)
- Adquirir e Implementar (AI)
- Entregar y dar Soporte (DS)
- Monitorear y Evaluar (ME)

Planear y Organizar

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio.

Adquirir e Implementar

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración 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.

Entregar y dar Soporte

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 operacionales. Se dan respuesta a las siguientes preguntas:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio? ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

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.

La Auditoría realizada a la Sección de Abastecimiento se centrara a dar cumplimiento al dominio denominado Entregar y Dar Soporte, como referencia general. Pues en el encontramos controles relacionados con seguridad, entrega de servicios que reflejan la naturaliza del proceso realizado.

2. Políticas de Seguridad para el Sector Salud MINSAL

El documento emana del ministerio de salud y es producto del trabajo realizado en el marco del desarrollo del proyecto "Política de Seguridad para Acceso a Redes e Información", comprendido en el ámbito de cumplimiento de la normativa del PMG (Programa para el Mejoramiento de la Gestión) Gobierno Electrónico para el año 2008.
La actual normativa por la cual debiese regirse el sector salud se encuentra consignada en el documento "Políticas de Seguridad para el Sector Salud, Octubre 2005" el cual abarca el tema de la seguridad en forma global.

Este documento plantea una revisión de la normativa mencionada, la cual se basa en la norma internacional ISO-IEC 27001, pero se limita a tratar los temas de Seguridad Física y de Acceso a Redes.
Los cambios propuestos al documento del año 2005 son los siguientes:

- Reordenar y Completar el Capítulo "Seguridad Física de las Instalaciones".
- Reordenar y Completar el Capítulo "Seguridad de Acceso a Redes".
- Agregar un Capítulo "Controles de Seguridad y Gestión de la Continuidad".

La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Su objetivo es ayudar a proteger los activos de información y otorgar confianza a cualquiera de las partes interesadas, sobre todo a los usuarios. La norma adopta

un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

3. ISO /IEC 27001 (Internacional Organization for Standardization / Internacional Electrotechnical Comisión)

La norma ISO/IEC 27001 (Tecnología de Información , Técnicas de Seguridad, Sistema de Gestión de la Seguridad de la Información, Requerimientos), publicada en Octubre 2005, es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, utilizando la metodología PDCA, **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Ejemplo de este método es el aplicado en el proceso de Auditoría realizado:

- Planificar: Definición Procedimientos Controles de Seguridad, Procedimientos
- Hacer: Realizar Controles.
- Verificar: Analizar la información de los Controles.
- Actuar: Publicar resultados.

ANEXO II – CUESTIONARIOS

En este anexo se dan a conocer los cuestionarios confeccionados para la recolección de evidencia en las áreas auditadas. Estos se dividen en cuestionarios de carácter general, para todos los actores involucrados en el proceso de Auditoría, y de carácter específico que fueron elaborados recabar información más precisa.

1. Cuestionarios Generales

Seguridad

Realizados para evaluar los distintos niveles de implementación de políticas de seguridad.

1. La organización ha escrito documentos de políticas de seguridad de la información que son fácilmente accesibles para los usuarios.
2. Las políticas de seguridad definen claramente a los responsables de esta (ejecutivos, administradores, oficiales de seguridad, empleados).
3. Las políticas de seguridad incluyen los requerimientos necesarios para educar sobre la concienciación de la seguridad.
4. Los documentos de políticas de seguridad especifican requerimientos para control de acceso lógico, incluyendo nombre de usuario y administración de passwords para aplicaciones y S.O.
5. Las políticas de seguridad indica las directrices para la seguridad física y del ambiente, incluyendo el acceso a edificios y visitantes no supervisados.
6. Las políticas de seguridad indican como proteger la privacidad de los datos de los clientes y empleados.
7. Las políticas de seguridad cubren reportes de incidentes y respuestas a los mismos.
8. Las políticas de seguridad contemplan los requerimientos para la continuidad del negocio, incluyendo el desarrollo y prueba del plan de recuperación.
9. Las políticas de seguridad cumplen con los requerimientos legales.

Información sobre herramientas de seguridad existentes en la red

Tiene como objetivo saber cuales medidas de seguridad mantiene la institución.

¿El siguiente Equipamiento/Software de seguridad está instalado en su establecimiento?

- Firewall.
- Servidores Antivirus
- Anti-spam de correos.
- Antivirus en los computadores de los usuarios.
- Firewalls en los computadores de usuarios.
- Herramientas de manejo de parches de Sistema Operativo centralizados.
- Sistemas centralizados de distribución de actualizaciones de antivirus.
- Filtrado de URLs.
- Antivirus para HTTP y SMTP, para evitar malware.

Sistemas de Información

1. ¿Cuáles son los Sistemas de Información que gobiernan los procesos realizados en la Sección de Abastecimiento del HCHM?
2. Como son llevados a cabo las capacitaciones para el personal nuevo en la organización. Quien es el responsable de llevarlas a cabo y como se controlan.
3. Los Sistemas de Información utilizados responden a los requerimientos actuales del área.
4. Se han planteado mejoras a los sistemas que permitan dar cumplimiento a los requerimientos.
5. Están al tanto del plan informático de la institución.
6. Se están realizando los proyectos según el plan informático.
7. Participan en la captura de requerimiento de los nuevos Sistemas de Información desarrollados.

Dispositivos de Almacenamiento

Este cuestionario tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos, Hardware, de almacenamiento de información.

1. La sala de servidores de datos tiene:

- Aire acondicionado
- Protección contra el fuego, indique
- Cerradura doble cierre
- Otra

2. ¿Tienen los servidores de datos protección automática contra el fuego?

Señalar de que tipo.

3. ¿Se verifican con frecuencia la validez de los inventarios de los respaldos?

4. ¿Existe un control estricto de las copias de respaldo?

5. ¿Que medio se utiliza para almacenarlos?

- Mueble con cerradura
- Bóveda

Otro, especifique.

6. Este lugar de almacenamiento se encuentra:

- En el mismo edificio donde se sitúan los servidores
- En otro lugar. Indique cual.

7. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

8. ¿Se certifica la destrucción o baja de los archivos defectuosos?

9 ¿Se tiene un responsable, por turno, de los servidores de datos?

10. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

11. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

12. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

13. ¿Existe un responsable en caso de falla?

14. ¿Se rotulan adecuadamente las copias de seguridad?

Mantenimiento

Este cuestionario tiene como objetivo evaluar las tareas correspondientes al mantenimiento del activo informático.

1. ¿Que tipo de mantenimientos se llevan a cabo?

2. ¿Existen mantenimientos de carácter preventivos. Con que frecuencia se realizan?

3. Existe un contrato de mantención con empresas externas a la institución.
4. Existen seguros o garantías contratadas.
5. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el
6. Se realiza mantenimiento periódico a los dispositivos de respaldo.
6. ¿Cómo se notifican las fallas?
7. ¿Cómo se les da seguimiento?

Funcionamiento de la Sala de Servidores

Este tiene como objetivo evaluar el correcto funcionamiento, así como la organización de la sala de servidores.

1. Existe un lugar asignado a las cintas y discos magnéticos?
2. ¿Se tiene asignado un lugar especifico para papelería y utensilios de trabajo?
3. ¿Se cuenta con el espacio suficiente en la sala de servidores?
4. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el Área de Soporte de Comunicaciones y la sala de servidores?
5. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?
6. Que operaciones realiza el personal ajeno al área en la sala de servidores.

Seguridad Física

Este cuestionario verifica la seguridad física de las instalaciones que utiliza la Sección de Abastecimiento, el Área de Soporte de Comunicaciones y la Oficina de Ingeniería de Sistemas, ya que de esto depende la continuidad de los servicios que prestan las áreas a la organización.

Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad física en el área?
2. ¿Qué tipos de medidas están implementadas?
3. ¿Existen una persona responsable de la seguridad?
4. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
5. ¿Existe personal de seguridad dedicado para el área?

6. ¿Cómo se controla el acceso al área?
7. ¿Existe personal de seguridad vigilando las 24 horas?
8. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
9. Se ha instruido a los funcionarios sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización.
10. Existen medidas de seguridad para prevenir desastres como:
    - Inundación
    - Terremoto
    - Fuego
11. Se cuenta con extintores en caso de incendio.
12. ¿Se ha capacitado al personal en el manejo de los extintores.
13. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
14. ¿Se ha capacitado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
15. Se ha prohíbe a los funcionarios el consumo de alimentos y bebidas en el interior del área.
16. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
17. ¿Las Actuales medidas de seguridad son las suficientes?

Cuestionario de Aceptación de los Sistemas

Tiene por objetivo conocer la opinión de los usuarios de los sistemas relacionado con el nivel de satisfacción que estos tiene, si facilitan el desarrollo de sus tareas y como poder mejorarlos.

1. ¿Los Sistemas de Información utilizados cuentan con manuales de usuario?
2. Estos manuales son claros y explicativos, son específicos del área.
3. Existe una capacitación formal de los sistemas a utilizar, quien las realiza y como se supervisa.
4. Los Sistemas de Información utilizados satisfacen los requerimientos actuales.
5. De no ser así se han planteado las mejoras.

6. Han participado en la captura de requerimientos de los nuevos Sistemas de Información o actualización de los actuales.
7. Han participado en capacitaciones de los nuevos Sistemas de Información o actualizaciones de los vigentes.
8. Podría mencionar los nuevos requerimientos que usted estima necesario se contemplen implementar.

Cuestionario Seguridad Lógica

1. ¿Qué medida de seguridad se han implementado para los diferentes sistemas?
2. Existen cuentas únicas para el acceso a los Sistemas de Información.
3. Existe una política clara para la utilización de los Sistemas de Información, relacionada con la explotación y seguridad.
4. ¿Quién controla que esta política se ejecute?
5. Se han registrado incidentes de acceso desde el exterior a los Sistemas de Información.
6. Se mantiene un registro de los incidentes producidos en los Sistemas de Información.
7. Se mantiene un registro de los errores cometidos por los usuarios de los sistemas.
8. Los equipos computacionales cuenta con Software antivirus.

2. Cuestionarios Específicos

Cuestionario Procedimiento de Despacho

Tiene como objetivo conocer el funcionamiento del proceso de despacho, actividades, personal que participa, controles.

1. ¿Cuáles son los pasos a seguir para efectuar un despacho ordinario?
2. Explique los estados del despacho.
3. ¿Cuáles son los estados que indican que un despacho contiene errores?
4. ¿Cómo se procede en caso de detectar errores en algún despacho?
5. Que documentos acompañan a un despacho.
6. ¿Cuál es el encargado de realizar los despachos, quien supervisa?

7. Como se cargan los productos a despachar al sistema, de forma automatizada o manualmente.
8. Como se lleva a cabo el proceso de devolución de parte de una unidad, y como se refleja en el sistema.
9. Como se gestionan los préstamos a otros servicios de salud.
10. Como se procesa un pedido de urgencia.
11. En caso de necesitar algún insumo por parte de una unidad fuera de turno como se procede.
12. Que se hace para prevenir que las unidades queden desabastecidas.
13. Como se procede al detectar la falta de algún insumo.
14. Como se procede al detectar que un producto se encuentra bajo su stock crítico.
15. Como se maneja el inventario.
16. Bajo que criterio se consumen los productos.
17. Como se procede al detectar que la información que indica el sistema no concuerda con la real.
18. Los requerimientos actuales son cubiertos por el sistema ANITA.
19. Se han planteado mejoras al sistema para mejorar el procedimiento de compra.

Cuestionario Procedimiento de Compra

Tiene como objetivo conocer el funcionamiento del proceso de Compra, actividades, personal que participa, controles.

1. ¿Cuáles son los pasos a seguir para efectuar una compra ordinaria?
2. Explique los estados de una compra.
3. ¿Cuáles son los estados que indican que una compra presenta errores?
4. ¿Cómo se procede en caso de detectar errores en los pedidos?
5. Como se ejecuta el plan de compras.
6. Como se elabora el plan anual de compras, quienes participan
7. Como se cargan los productos al sistema, de forma automatizada o manualmente.
8. Como se procesan los pedidos extraordinarios no contemplados en el plan de compras.

9. Los pedidos deben replicarse de forma manual en el portal chile compra, o se cargan automáticamente desde el Sistema ANITA.
10. Los requerimientos actuales son cubiertos por el Sistema ANITA.
11. Se han planteado mejoras al sistema para mejorar el procedimiento de compra.

Cuestionario Procedimiento de Recepción

Tiene como objetivo conocer el funcionamiento del proceso de Recepción, actividades, personal que participa, controles.

1. ¿Cuáles son los pasos a seguir para efectuar una recepción?
2. Explique los estados del despacho.
3. ¿Cuáles son los estados que indican que un despacho contiene errores?
4. ¿Cómo se procede en caso de detectar errores en algún despacho?
5. Que documentos acompañan a un despacho.
6. ¿Cuál es el encargado de realizar los despachos, quien supervisa?
7. Como se cargan los productos a despachar al sistema, de forma automatizada o manualmente.
8. Como se lleva a cabo el proceso de devolución de parte de una unidad, y como se refleja en el sistema.
9. Como se gestionan los préstamos a otros servicios de salud.
10. Como se procesa un pedido de urgencia.
11. En caso de necesitar algún insumo por parte de una unidad fuera de turno como se procede.
12. Que se hace para prevenir que las unidades queden desabastecidas
13. Los requerimientos actuales son cubiertos por el sistema ANITA.
14. Se han planteado mejoras al sistema para mejorar el procedimiento de compra.

Cuestionario Procedimiento de Baja de Productos

Tiene como objetivo conocer el funcionamiento del proceso de baja de productos, actividades, personal que participa, controles.

1. ¿Cuáles son los pasos a seguir para dar de baja un producto?
2. Cuales son los criterios usados para dar de baja un producto.

3. Quienes son los responsables de ejecutar el proceso.
4. Que documentos acompañan a una baja de productos.
5. Como se refleja esta baja en el sistema.

Cuestionario Área de Soporte de Comunicaciones – Servidores

1. ¿Cuantos servidores existen en la salda de computo?
2. ¿Qué Sistemas de Información y aplicaciones corren en ellos?
3. ¿Cuáles son las características técnicas del servidor que soporta el sistema base?
4. ¿Qué tipo de mantenciones son realizadas en los servidores?
5. ¿Cómo se procede ante una emergencia en los servidores?
6. ¿En caso de una emergencia fuera de turno, como se procede?
7. ¿Existen seguros comprometidos para los servidores, y para cuales de ellos?
8. ¿Cuentan con UPS independiente cada uno de los servidores?
9. Cree usted que las características técnicas del servidor base cumple con los requerimientos actuales para dar un servicio eficiente.
10. La sala de servidores se encuentra debidamente ventilada.
11. Existen sensores de temperatura, humedad, humo en la sala de servidores.
12. Cuentan la sala de servidores con extintores.
13. En caso de una perdida del suministro eléctrico ¿Los servidores pueden seguir operando?

Cuestionario Sistema HERMINDA

1. ¿Cómo funciona el Sistema HERMINDA?
2. ¿Qué lenguaje es fue utilizado en si desarrollo, que tipo de base de datos se utiliza?
3. El sistema fue desarrollo internamente por la Sección de Abastecimiento.
4. Como se respalda la información del Sistema HERMINDA y quien la realiza.
5. En caso de producirse un error quien es el encargado de volver el servicio operativo nuevamente.
6. El sistema se encuentra debidamente documentado.
7. Se ha elaborado un manual de usuario del sistema, quien lo confecciono.

8. Se controla el uso correcto del sistema, se mantienen informes de los errores producidos.
9. Cual es el procedimiento para registrar un nuevo usuario.
10. Cual es el procedimiento para dar de baja a un usuario.
11. Cual es método de autentificación utilizado por el sistema.
12. Existen cuentas únicas en los sistemas.
13. Existen perfiles definidos en el sistema.
14. Se mantiene una política de cambio de contraseñas permanente.
15. Existe un procedimiento que indique la composición que debe tener la contraseña.
16. El sistema se bloquea ante un ingreso erróneo reiterado.
17. La información se encuentra cifrada.
18. Son llevados a cabo mantenimientos permanentes al sistema.
19. Se han planteado realizar mejorar al sistema.
20. Se han registrado intentos de acceder desde el exterior hacia el sistema. Existen medidas de seguridad para protegerse de aquello.

Cuestionario Sistema ANITA

1. ¿Cuáles son las características Sistema ANITA?
2. ¿Qué lenguaje es fue utilizado en si desarrollo, que tipo de base de datos se utiliza?
3. ¿Cuáles son las funcionalidades del Sistema ANITA?
4. Como se respalda la información del Sistema ANITA y quien la realiza.
5. Quien es el administrador del sistema.
6. En caso de producirse un error quien es el encargado de volver el servicio operativo nuevamente.
7. El sistema se encuentra debidamente documentado.
8. Se ha elaborado un manual de usuario del sistema, quien lo confecciono.
9. Se controla el uso correcto del sistema, se mantienen informes de los errores producidos.
10. Cual es método de autentificación utilizado por el sistema.
11. Existen cuentas únicas en los sistemas.
12. Existen perfiles definidos en el sistema.

13. Los perfiles actuales son los adecuados para los requerimientos de hoy.
14. Cual es el procedimiento para registrar un nuevo usuario.
15. Cual es el procedimiento para dar de baja a un usuario.
16. Se exige el cambio de contraseña en el primer ingreso de un usuario nuevo.
17. Se mantiene una política de cambio de contraseñas permanente.
18. Existe un procedimiento que indique la composición que debe tener la contraseña.
19. El sistema se bloquea ante un ingreso erróneo reiterado.
20. La información personal de los usuarios se encuentra cifrada.
21. La información almacenada se encuentra cifrada.
22. Son llevados a cabo mantenimientos permanentes al sistema.
23. Se han planteado realizar mejoras al sistema.
24. Se realizan capacitaciones a los usuarios del sistema.
25. Que mejoras se han realizado en el sistema hasta la fecha.

ANEXO III – ENTREVISTAS

Entrevista 1

Nombre: Raúl Vielma

Cargo: Jefe de la Sección de Abastecimiento

1. ¿Cómo esta organizado el área?
    - ¿Cuántas personas trabajan?
    - ¿Cómo se organizan los turnos de trabajo?
    - ¿Cuáles son las personas que tienen acceso a los Sistemas de Información?
    - ¿El área ha sido auditada previamente?

2. ¿Qué sistemas de seguridad existen para el área?
    - Existe personal de seguridad exclusivo
    - Existe controles de ingreso al área (Físico).
3. ¿Cuántos Sistemas de Información existen dentro de la Sección?
    - ¿Qué función desempeña cada uno?
    - ¿Estos sistemas son propios de este hospital, son utilizados en otros hospitales?
    - ¿En que año se implemento cada uno?
    - ¿Con que otras áreas y/o sistemas del hospital interactúan?
    - ¿Cual es el personal encargado de ingresar datos al sistema?
    - ¿Qué tipos de reportes y con frecuencia se emiten y a quienes van dirigidos?
    - Mediante que técnicas se controla el acceso lógico.

4. ¿Existe alguna planificación para la manutención de los Sistemas de Información?
    - Esta tarea es realizada por personal externo o interno
    - ¿Existe documentación de los sistemas?
    - ¿Se mantiene algún registro histórico de los errores presentados por los sistemas?
    - ¿Existen procedimientos para la adquisición de nuevas piezas por reparación o actualización de los sistemas?

5. Existen políticas de respaldo de los sistemas
    - ¿Qué dispositivos se utilizan?
    - ¿Con qué frecuencia se realiza el respaldo?
    - ¿Quién es el encargado de realizar el respaldo?
    - ¿Quién lo supervisa?
    - ¿Donde se almacena?
    - ¿Cuanto tiempo se almacena?
    - ¿Se encuentra debidamente rotulado?
    - ¿Cuantas copias se almacenan y donde se almacenan?

6. ¿Hay procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de desastres o contingencias?
    - Se cuenta con suministro de electricidad de emergencia.
    - Cuando se restablecen los sistemas como se traspasa la información generada y quien es el encargado.
    - Indicar Fallos considerables que a presentado el sistema

7. El acceso a las bodegas se encuentra restringido
    - ¿Quién es el personal encargado?
    - ¿Como se realiza el proceso de suministros para las diferentes áreas?
    - ¿Qué políticas se utilizan para la adquisición de los insumos?
    - ¿Qué método de control stock utilizan?

Entrevista 2

Nombre: Raúl Vielma

Cargo: Jefe de la Sección de Abastecimiento

Cuestionario Sección Abastecimiento

Objetivo: Comprobar medidas seguridad por parte de los directivos.

1. ¿Se ha adoptado medidas de seguridad para los equipos y sistemas por parte de la dirección? Si/No
2. ¿Existe una persona responsable de la seguridad computacional dentro del área? Si/No
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad? Si/No
4. Existen cuentas únicas para cada persona en los diferentes sistemas.
5. Se mantiene una política de cambio de claves y con que frecuencia se realiza.
6. Quien verifica el cumplimiento de estas políticas
7. ¿Se controla el trabajo fuera de horario? Si/No
8. ¿Se registran las acciones de los operadores para evitar que realicen alguna operación que pueda dañar el sistema? Si/No

Cuestionario Procedimientos

Objetivo: Comprobar desempeño del área en contingencia

1. Cuanto tiempo tardan en resolverse las solicitudes de abastecimiento desde las diferentes áreas.
2. Los requerimientos de las diferentes áreas son realizadas vía sistema.
3. Como se manejan las solicitudes de abastamiento y las salidas de bodega cuando los sistemas se encuentran interrumpidos.
4. Existen algún reglamento para las solicitudes de emergencia desde las diferentes unidades del hospital.(urgencia)
5. Como se manejan las compras de adicionales no contempladas en el presupuesto anual.

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

1. Quienes participan en el proceso de desarrollo de un nuevo sistema.
2. Que documentación es la que acompaña a un sistema cuando se entrega.
3. Se realizan capacitaciones adicionales a la documentación entregada.
4. Se llevan a cabo revisiones para determinar si los sistemas cumplen con los objetivos para los que fueron diseñados.
5. Se lleva a cabo algún tipo de evaluación que verifique el manejo de los sistemas por parte de los nuevos usuarios.
6. Los manuales entregan la información que se adecue a las necesidades de los nuevos usuarios.

Entrevista 3

Entrevistado: Roller Sanchez

Cargo: Jefe Unidad de Compras

Cuestionario Procedimientos.

Objetivo: Comprobar el desempeño del área respecto a las políticas establecidas por la dirección.

1. Descripción del cargo; responsabilidades, funciones, personal a cargo, jefe.
2. Cuales son los Sistemas de Información que la unidad de compra utiliza
3. Como se elabora el plan anual de compras, cual es su rol y como se ejecuta.
4. Quien controla la ejecución de este plan de compras.
5. Como se lleva a cabo una compra ordinaria, mencione los pasos seguidos, estados, controles efectuados.
6. Como se realizan las compras no contempladas en el plan de compras. Existen formularios para este tipo de compra
7. Como se maneja la criticidad de los insumos relacionados con el stock.

8. Como se procede al detectar un error en el proceso de compra, a quien se informa, como se corrige.
9. Como se gestiona la devolución de algún insumo.
10. Se registran los errores que se producen.
11. Como funciona la unidad en la eventualidad de no contar con los Sistemas de Información.
12. Que persona es la encargada de subrogarlo en caso de ausentarse.

Cuestionario Seguridad

Objetivo: Comprobar medidas seguridad por parte de los directivos.

13. Que medidas de seguridad se han adoptado para salvaguardar la integridad del equipamiento computacional, documentación en la sección.
14. Estos tipos de controles de seguridad se encuentran detallados en un manual de procedimientos.
15. Como se controla el acceso a los diferentes Sistemas de Información utilizados en la sección.
16. Que tipo de perfiles de usuarios existen en la Unidad.
17. Existe alguna restricción para el ingreso erróneo reiterado de los usuarios a los sistemas.
18. Se exige el cambio de claves por defecto al ingresar por primera vez a cada uno de los Sistemas de Información.
19. Existe alguna restricción en la composición de las claves de acceso a los diferentes Sistemas de Información.
20. Existe y se lleva a cabo una política de cambio de claves.
21. Existen cuentas únicas para cada persona en los diferentes sistemas.
22. Se mantiene una política de cambio de claves y con que frecuencia se realiza.
23. Quien verifica el cumplimiento de estas políticas.
24. En su opinión. Las actuales medidas de seguridad son las adecuadas para proteger la información que se maneja, el equipamiento de la sección.
25. Se han planteado nuevas medidas de seguridad física o lógica para la unidad o sección.

26. ¿Se registran las acciones de los operadores para evitar que realicen alguna operación que pueda dañar el sistema?

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

27. Existen manuales de uso de los Sistemas de Información utilizados en el área.
28. El personal se rige por estos manuales y quien controla que así se realice.
29. Los manuales entregan la información que se adecue a las necesidades de los nuevos usuarios.
30. Se han desarrollado nuevas funcionalidades para la sección y/o unidad en el último tiempo, podría mencionarlas y describirlas brevemente.
31. Han participado en la captura de requerimiento de estas nuevas funcionalidades y en que forma.
32. Se han efectuado capacitaciones al personal para la utilización de estas funcionalidades.
33. En caso del nuevo personal, quien es el encargado de capacitarlo en la utilización de los Sistemas de Información.
34. Se llevan a cabo revisiones para determinar si los sistemas cumplen con los objetivos para los que fueron diseñados.
35. Se lleva a cabo algún tipo de evaluación que verifique el manejo de los sistemas por parte de los nuevos usuarios.
36. Se han efectuado recomendaciones para nuevas funcionalidades a desarrollar, para un mejor desempeño de la sección o unidad.

Entrevista 4

Nombre: Marisol Fernández

Cargo: Jefe Área de Soporte de Comunicaciones

Cuestionario Seguridad Física.

1. ¿Se ha adoptado medidas de seguridad por parte de la dirección de informática? ¿Si/No/Explique?
2. ¿Existe una persona responsable de la seguridad computacional dentro del área? Si/No
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad? Si/No
4. ¿Se controla el trabajo fuera de horario? Si/No
5. ¿Se registran las acciones de los operadores para evitar que realicen alguna operación que pueda dañar el sistema? Si/No
6. ¿ Se controla la entrada al lugar donde se encuentran servidores y equipos
7. El lugar donde se ubican los equipos esta seguro de siniestros que puedan poner en peligro los equipos y/o información.
8. ¿Se ha instruido a personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? Si/No
9. Existe espacio suficiente para los equipos y servidores.
10. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del cuarto de máquinas para evitar daños al equipo? Si/No
11. ¿Se garantiza el suministro eléctrico que permita bajar las aplicaciones de los servidores?
12. ¿Se posee un procedimiento automatizado para bajar las aplicaciones en caso de que el suministro eléctrico falle fuera de los horarios de trabajo?
13. ¿Se vigilan el comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
14. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos? Si/No
15. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora? Si/No
16. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad, etc.) que garantice su integridad en caso de que ocurra algún siniestro.
17. ¿Se tienen establecidos procedimientos de actualización a estas copias? Si/No

Cuestionario Procedimientos

1. ¿Qué información es la que se respalda?
2. ¿Cómo se verifica la validez de los respaldos?
3. ¿En caso de existir discrepancias en el contenido de los diferentes respaldos como se resuelve?
4. ¿Con que frecuencia se presentan discrepancias?
5. ¿Se tiene algún procedimiento para restituir la información perdida?
6. ¿Se tiene identificados los archivos que cuentan con información confidencial y se cuenta con claves de acceso?
7. ¿Existe un control estricto para el manejo de los diferentes respaldos de la información confidencial?
8. ¿Se certifica la eliminación de los archivos que se encuentren defectuosos?
9. ¿Qué medidas se toman en caso del extravió de algún dispositivo de almacenamiento?
10. ¿Existe algún procedimiento que se utilice para registrar los archivos/dispositivo que se prestan a otras áreas?
11. ¿Cómo se realiza el reemplazo de los respaldos en cintas?
12. ¿Se controla que la cinta que permanecerá antes de la eliminación de la anterior (información)?
13. ¿Se tiene restringida la operación del los servidores solo al personal del área?
14. ¿Se tiene implantada una política de cambio de claves cada cierto tiempo o en caso de que llegue personal nuevo al área?

Entrevista 5

Entrevistada: Marisol Fernández

Cargo: Jefa Área de Soporte de Comunicaciones.

Cuestionario Procedimientos

Objetivos: Comprobar el desempeño del área respecto a las responsabilidades establecidas.

1. Descripción de la sección, como se encuentra organizada, cuanto personal trabaja, descripción de su cargo y las funciones que desempeña.
2. ¿Cuáles son los Sistemas de Información que la sección administra y que funciones se desempeñan en dicha tarea?
3. ¿Qué Sistemas de Información utilizan como usuarios y que personas lo hacen, bajo que perfiles?
4. Se encuentran detalladas las funcionalidades y responsabilidades del área, los usuarios se apegan a ellas.
5. Requiere del personal de otras áreas para dar cumplimiento a algunas funciones. Indique cuales.
6. La cantidad de personal es la adecuada para dar cumplimiento a todas las responsabilidades.

Cuestionario Sistemas de Información

Objetivos: Conocer los Sistemas de Información utilizados, características y funciones.

7. Podría describirnos el Sistema ANITA, los módulos que la componen:
   - SAM (Sistema de Atención Médica)
   - ABASUR (Abastecimiento Sur)
   - FINANZAS
   - FARMACIA

8. De administrar otros Sistemas de Información solicitar que los describa.

9. ¿Quién es el responsable del ingreso del catálogo de insumos al Sistema ANITA. Y quien es el encargado de proporcionar esta información?
10. Participan como unidad en el desarrollo de nuevas aplicaciones, de ser así, en qué forma.
11. Se ha indicado que existe replicación de información, por que sucede esto y que sistemas se encuentran involucrados.
12. ¿Cuantos usuarios aproximadamente utilizan los distintos Sistemas de Información?
13. ¿Qué tipos de bases de datos son utilizados por los diferentes Sistemas de Información?
14. ¿Bajo qué tipo de cifrado se encuentra la información almacenada en las bases de datos?
15. Cree Ud. Que los requerimientos del Sistema ANITA han cambiado en la actualidad, de ser así que medidas se han tomado para dar cumplimiento a ellas.
16. Se encuentra entre los futuros proyectos desarrollar o adquirir un nuevo sistema base, o adquirir uno, que responda a los requerimientos actuales.
17. ¿Existe algún procedimiento formal tanto para dar de alta como para dar de baja a algún usuario, podría detallarlos?

Cuestionarios Servidores

Objetivos: Verificar la seguridad de la sala de servidores, uso y respaldos de información.

18. Podría indicarnos la cantidad de servidores existentes, y que aplicaciones corren en ellos.
19. ¿Qué servidores cuentan con UPS?
20. La sala de servidores se encuentra debidamente ventilada.
21. ¿Existen extintores u otras medidas de prevención de siniestros en la sala de servidores u oficina?
22. ¿Como se controla el acceso a los servidores. Se tiene restringido el acceso sólo a personal del área?
23. Los actuales servidores cumplen con los requerimientos para correr de manera eficiente las aplicaciones. De no ser así se han planteado recomendaciones.
24. Estima Ud. Que la salda de servidores se encuentra bien emplazada. Existen planes para un cambio de ubicación.
25. Existe algún inconveniente de mantener en un mismo lugar los servidores de la Oficina de Ingeniería de Sistemas.
26. Se realizan mantenciones a los servidores, con qué frecuencia y bajo que circunstancias.

27. Estima Ud. Que las medidas de seguridad son las apropiadas para salvaguardar el equipamiento y la información que en ellos se almacena.

Cuestionario Seguridad Física y lógica.

Objetivo: Comprobar medidas seguridad presentes en la unidad.

28. Se ha finalizado la elaboración del manual de seguridad indicado con anterioridad. Se pretende difundirlo al resto del hospital y quien lo haría de ser así.
29. Cuán importante estima Ud. Que es la seguridad para el área. Cuál cree que es la opinión de la dirección.
30. ¿ Se controla la entrada al lugar donde se encuentran servidores y equipos
31. Se registran las acciones erróneas de los usuarios en los Sistemas de Información.
32. Que aspectos sugeriría Ud. Que puedan mejorarse, no sólo hablando de la seguridad.
33. Se cuenta con una política de cambio de claves permanente. Quien verifica el cumplimiento de estas políticas. De no ser así se ha sugerido de parte de la sección que así se realice.
34. Existe alguna restricción para el ingreso erróneo reiterado de los usuarios a los sistemas.
35. Se exige el cambio de claves por defecto al ingresar por primera vez a cada uno de los Sistemas de Información.
36. ¿Existe alguna restricción en la composición de las claves de acceso a los diferentes Sistemas de Información?
37. ¿Existe espacio suficiente para los equipos y servidores?
38. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del cuarto de máquinas para evitar daños al equipo?
39. ¿Se tienen aislados los servidores de materiales considerados combustibles?
40. ¿Se garantiza el suministro eléctrico que permita bajar las aplicaciones de los servidores?
41. ¿Se posee un procedimiento automatizado para bajar las aplicaciones en caso de que el suministro eléctrico falle fuera de los horarios de trabajo?
42. ¿Cuál es el procedimiento para dar de alta y dar de baja a un nuevo usuario?

43. Se cuenta con una política de cambio de claves permanente. Quien verifica el cumplimiento de estas políticas. De no ser así se ha sugerido de parte de la sección que así se realice.
44. ¿Existe alguna restricción para el ingreso erróneo reiterado de los usuarios a los sistemas?
45. Se exige el cambio de claves por defecto al ingresar por primera vez a cada uno de los Sistemas de Información.
46. Existe alguna restricción en la composición de las claves de acceso a los diferentes Sistemas de Información.
47. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
48. ¿Se cuenta con seguros que respalden el Software y Hardware de los servidores principales? (Ante que siniestros responden y que plazos se tienen establecidos)
49. Se han producido ataques a los Sistemas de Información desde el exterior.
50. Existen medidas de seguridad que permitan proteger los Sistemas de Información de ataques desde el exterior.
51. Se registran los errores de los usuarios en los sistemas. Quien los analiza y como se controlan.
52. ¿Cuáles son los errores que se presentan con mayor frecuencia por parte de los usuarios?

Cuestionario Respaldos

Objetivos: Verificar la existencia, la frecuencia y el tipo de respaldo realizado, y el resguardo que se mantiene de ellos.

53. ¿Qué respaldos se llevan a cabo, a que Sistemas de Información y de qué tipo?
54. ¿Con qué frecuencia se llevan a cabo, indique días de la semana?
55. ¿Como es el procedimiento realizado para realizar las copias de respaldo, como se rotulan?
56. Estima Ud. Que la frecuencia es la más apropiada para salvaguardar la información. De no ser así que plantea Ud.
57. ¿Cuantas copias de seguridad se realizan, bajo que soporte físico se realizan?

58. ¿Qué información es la que se respalda?
59. ¿Cómo se verifica la validez de los respaldos? Como se procede al identificar la no validez de alguna copia.
60. Se han presentado instancias en que deba restaurarse completamente las bases de datos. Cuánto tiempo tarda en restaurar la información desde un respaldo.
61. De encontrarse dañada alguna copia de respaldo, como se procede para recuperar dicha información.
62. Como es el procedimiento para dar de baja algún medio de respaldo. Se realiza algún procedimiento especial antes de eliminarlo.
63. En caso del extravió de algún respaldo, como se procedería.
64. ¿Se controla que la cinta que permanecerá antes de la eliminación de la anterior (información)?
65. ¿Se tiene restringida la operación del los servidores solo al personal del área?

Cuestionario Continuidad de Operaciones

Objetivo: Verificar que existan medidas para garantizar la continuidad del servicio.

66. En el caso de una caída de los sistemas bajo su administración quien o quienes se encargan de volverlos operativos nuevamente.
67. Que persona es la encargada de subrogarlo en caso de ausentarse. De contar con uno, esta persona tiene los permisos suficientes para cumplir cabalmente su función.

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

68. Participan en el proceso de desarrollo de un nuevo sistema o modificación de uno ya existente. ¿En que consiste la participación?

69. Todos los Sistemas de Información cuentan con manuales de uso, son lo suficientemente informativos, podrían mejorarse.
70. Participan en las capacitaciones o en la confección de los manuales de nuevas aplicaciones
71. Existen la instancia en que los usuarios planteen mejoras a los sistemas actuales.
72. Cree Ud. Que el Sistema ANITA responde a los requerimientos actuales. De no ser así que nuevos requerimientos debiese satisfacer.

Entrevista 6

Entrevistado: Ingrid Vergara

Cargo: Jefa Bodega

Cuestionario Procedimientos.

Objetivo: Comprobar el desempeño del área respecto a las políticas establecidas por la dirección.

1. Descripción del Unidad, que tipos de bodegas existen, personal que trabaja, horarios, organización y funciones que desempeñan
2. Descripción del cargo; responsabilidades, jefe directo.
3. ¿Cuáles son los Sistemas de Información que la unidad utiliza. Y qué tipo de perfiles utilizan?
4. Qué persona es la encargada de subrogarlo en caso de ausentarse. De contar con uno, esta persona tiene los permisos suficientes para cumplir cabalmente su función.
5. ¿Qué funciones cumple la unidad en la ejecución del plan anual de compras?
6. ¿Qué tipo de despachos son efectuados en la unidad, con qué frecuencia?
7. ¿Como se procesa un pedido ordinario? ¿Que información es ingresada al sistema?
8. ¿Como se procesa un pedido que no se encuentra en la planificación?
9. ¿Como se procesa un pedido de emergencia?
10. ¿Como se procesa una recepción en la unidad? ¿Que información es la ingresada al sistema?

11. Cuál es el procedimiento al detectarse un error en el proceso de despacho, a quien se informa, y como se corrige.
12. Cuál es el procedimiento al detectarse un error en el proceso de recepción, a quien se informa, y como se corrige.
13. Los errores que se producen son registrados en el sistema.
14. ¿Cómo se ingresan los productos cuando se recepcionan? Existe un proceso automatizado que permita mitigar los errores de un proceso manual.
15. ¿Qué medios son utilizados para que las unidades realicen sus pedidos? Existen pedidos automatizados mediante algún Sistema de Información.
16. ¿Como se maneja la criticidad de los insumos relacionados con el stock?
17. La distribución de los insumos se rigen bajo un criterio que exija
18. ¿Como se procede al detectar un error en el proceso de compra, a quien se informa, como se corrige?
19. ¿Como se gestiona la devolución de algún insumo?
20. Se registran los errores que se producen tanto en el despacho, como en la recepción de insumos.
21. ¿Cómo funciona la unidad en la eventualidad de no contar con los Sistemas de Información?
22. ¿Qué persona es la encargada de subrogarlo en caso de ausentarse?
23. ¿Con qué frecuencia se llevan a cabo controles de inventario?
24. ¿Como se procede al detectar que la información que entrega el Sistema ANITA no concuerda con la real?
25. Como se procede al detectar la ausencia de algún insumo o si este se encuentra bajo su stock crítico. Se ha presentado una situación así.
26. Cual fueron los motivos que impulsaron la fusión de las bodegas General y Farmacia. Se incluye la Bodega de Intangibles.
27. ¿Como se procede en caso de las mermas de insumos, sea estas por caducidad o pérdida?
28. ¿Como se procede al detectar que una unidad realiza un pedido que exceda lo planificado para ella?

29. ¿Cómo se manejan las solicitudes de abastamiento y las salidas de bodega cuando los sistemas se encuentran interrumpidos?
30. Existen algún reglamento para las solicitudes de emergencia desde las diferentes unidades del hospital.(urgencia)
31. ¿Cómo se gestionan los productos distribuidos y solicitados, que son rechazados por algún área?
32. Si una unidad necesitase algún insumo fuera del turno de bodega, como se procede.
33. ¿Cual es el procedimiento formal para dar de baja un insumo, y como se registra en el sistema?

Cuestionario Seguridad

Objetivo: Comprobar medidas seguridad y controles implantados en la unidad.

34. ¿Con que medidas de seguridad cuenta la Bodega que permita salvaguardar los insumos almacenados, el equipamiento y documentación?
35. ¿Como se controla el acceso físico a la unidad?
36. Existen controles, medidas para salvaguardar la bodega en caso de siniestros.
37. ¿Como se controla el acceso a los diferentes Sistemas de Información utilizados en la sección?
38. ¿Qué tipo de perfiles de usuarios existen en la Unidad?
39. Se les exige un cambio de claves permanente para el ingreso a los sistemas
40. En su opinión. Las actuales medidas de seguridad son las adecuadas para proteger la información, equipamiento e insumos.
41. Se han planteado nuevas medidas de seguridad física o lógica para la unidad o sección.

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

42. Los procedimientos que son seguidos por la unidad se encuentran detallados en algún manual. Se controla de alguna manera que se rijan por ellos.
43. Los manuales entregan la información clara y suficiente que permita un óptimo uso de los Sistemas de Información.
44. Se realizan capacitaciones para el personal nuevo. Quien es el responsable de realizarlas.
45. Los Sistemas de Información satisfacen los requerimientos de la unidad. Plantearía mejoras que optimizaran el trabajo.

Entrevista 7

Entrevistado: Gastón Vergara

Cargo: Jefe Oficina Ingeniería de Sistemas

Cuestionario Procedimientos

Objetivos: Comprobar el desempeño del área respecto a las responsabilidades establecidas.

1. Descripción de la sección, como se encuentra organizada, cuanto personal trabaja, descripción de su cargo y las funciones que desempeña.
2. Cuáles son los Sistemas de Información que la sección administra y que funciones se desempeñan en dicha tarea.
3. Que Sistemas de Información utilizan como usuarios y que personas lo hacen, bajo que perfil.
4. Existe algún procedimiento formal tanto para dar de alta como para dar de baja a algún usuario, podría detallarlos.
5. Quien es el responsable del ingreso del catálogo de insumos al Sistema ANITA.

Cuestionario Sistemas de Información

Objetivos: Conocer los Sistemas de Información utilizados, características y funciones.

6. Podría describirnos los módulos del Sistema ANITA, indicando a su vez el significado de sus siglas:
   - SAM
   - ABASUR
   - FINANZAS
   - FARMACIA

7. Descripción del Sistema HERMINDA, perfiles existentes y sus módulos:
   - Evaluación Costos Item 21,22.
   - Evaluación Productos Intermedios.
   - Tableros de mando Generales
   - Evaluación Estado Resultados C.R Finales

8. Podría describirnos el sistema de pedidos (desarrollados por alumnos de la UBB) que se encuentra implementado, lenguaje, tipo de base de datos, y con que sistemas interactúa. Y en qué porcentaje en relación a los métodos tradicionales es utilizado.
9. Se ha indicado que existe replicación de información, por que sucede esto y que sistemas se encuentran involucrados.
10. Qué factores son considerados relevantes a la hora de desarrollar alguna aplicación, seguridad, integridad de la información, confidencialidad de la información, confiabilidad, disponibilidad, mencione otros de estimarlo.
11. Cuantos usuarios aproximadamente utilizan los distintos Sistemas de Información.
12. Que tipos de bases de datos son utilizados por los diferentes Sistemas de Información
13. Bajo qué tipo de cifrado se encuentra la información almacenada en las bases de datos.
14. Todos los Sistemas de Información se encuentran debidamente documentados.
15. Existen aplicaciones a ser desarrolladas para la Sección de Abastecimiento, o relacionadas con el. De ser así podría describirlas.
16. Cree Ud. Que los requerimientos del Sistema ANITA han cambiado en la actualidad, de ser así que medidas se han tomado para dar cumplimiento a ellas.
17. Se encuentra entre los futuros proyectos desarrollar un nuevo sistema base, o adquirir uno, que responda a los requerimientos actuales.

18. En qué fase del desarrollo se encuentra la Plataforma utilizando códigos de barra para bodegas. Y para qué fecha se pretende tenerla operativa.
19. Que horizonte de evaluación tienen los Sistemas de Información, ANITA, HERMINDA y otros.
20. Que fases debe cumplir una nueva aplicación antes de estar completamente operativa.

Cuestionario Seguridad Física y Lógica

Objetivos: Comprobar la existencia de políticas, medidas, controles de seguridad Física y Lógica.

21. Se cuenta con una política de cambio de claves permanente. Quien verifica el cumplimiento de estas políticas. De no ser así se ha sugerido de parte de la sección que así se realice.
22. Existe alguna restricción para el ingreso erróneo reiterado de los usuarios a los sistemas.
23. Se exige el cambio de claves por defecto al ingresar por primera vez a cada uno de los Sistemas de Información.
24. Existe alguna restricción en la composición de las claves de acceso a los diferentes Sistemas de Información.
25. Cree Ud. Que La sala de servidores se encuentra bien ubicada, su emplazamiento genera algún inconveniente para su sección. De ser así se ha planteado aquella inquietud.
26. Cuáles cree Ud. Que son los errores que se producen con mayor frecuencia por parte de los usuarios de los sistemas. Se han planteado mejoras para solventarlos.
27. Se han producido ataques a los Sistemas de Información desde el exterior.
28. Existen medidas de seguridad que permitan proteger los Sistemas de Información de ataques desde el exterior.
29. Se registran los errores de los usuarios en los sistemas. Quien los analiza y como se controlan.
30. Cuáles son los errores que se presentan con mayor frecuencia por parte de los usuarios.
31. Qué medidas de seguridad o controles se han adoptado para salvaguardar la integridad del equipamiento computacional, documentación en la oficina.
32. De existir estos tipos de controles de seguridad se encuentran detallados en un manual de procedimientos.

33. Se han planteado nuevas medidas de seguridad física o lógica para la oficina, sala de servidores.

Cuestionario Continuidad de Operaciones

Objetivo: Verificar que existan medidas para garantizar la continuidad del servicio.

34. En el caso de una caída de los sistemas bajo su administración quien o quienes se encargan de volverlos operativos nuevamente.
35. Que persona es la encargada de subrogarlo en caso de ausentarse. De contar con uno, esta persona tiene los permisos suficientes para cumplir cabalmente su función.
36. En su opinión. Las actuales medidas de seguridad física o lógica en los Sistemas de Información son las adecuadas para proteger el equipamiento y la información que se maneja.
37. Los actuales servidores se desempeñan de forma eficiente o han presentado fallas. Se han planteado renovaciones.

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

38. Cuál es el personal del área encargado de llevar a cabo las capacitaciones para las nuevas aplicaciones.
39. Los Sistemas de Información cuentan con manuales de uso, se verifica que estos se ejecuten como se detalla en ellos.
40. Se ha evaluado el nivel de satisfacción de los usuarios en relación a los Sistemas de Información que se utilizan.
41. Existen instancias en que los usuarios puedan plantear sus consideraciones hacia los Sistemas de Información.
42. Los manuales de uso entregan toda la información requerida por parte de los usuarios para un óptimo uso.

43. Se llevan a cabo revisiones para determinar si los sistemas cumplen con los objetivos para los que fueron diseñados.

Entrevista 8

Entrevistado: Raúl Vielma

Cargo: Jefe de la Sección de Abastecimiento

Cuestionario Seguridad.

Objetivo: Comprobar medidas seguridad por parte de los directivos.

1. ¿Se ha adoptado medidas de seguridad para los equipos y sistemas por parte de la dirección? ¿Qué tipo de medidas y sobre que equipos?
2. ¿Existe un manual de procedimientos de seguridad para el área?
3. ¿Existe una persona responsable de la seguridad computacional dentro del área?
4. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
5. Existen cuentas únicas para cada persona en los diferentes sistemas.
6. Se mantiene una política de cambio de claves y con que frecuencia se realiza.
7. Quien verifica y como verifica el cumplimiento de estas políticas
8. ¿Se controla el trabajo fuera de horario?
9. ¿Se registran las acciones de los operadores para evitar que realicen alguna operación que pueda dañar el sistema?

Cuestionario Procedimientos

Objetivo: Comprobar desempeño del área en contingencia

10. Cuanto tiempo tardan en resolverse las solicitudes de abastecimiento desde las diferentes áreas.
11. Los requerimientos de las diferentes áreas son realizadas vía sistema.
12. Como se manejan las solicitudes de abastamiento y las salidas de bodega cuando los sistemas se encuentran interrumpidos.

13. Existen algún reglamento para las solicitudes de emergencia desde las diferentes unidades del hospital.(urgencia)
14. Como se manejan las compras de adicionales no contempladas en el presupuesto anual.

Cuestionario Aceptación Sistemas

Objetivos: Verificar Aceptación por parte de los usuarios de los nuevos sistemas o módulos implantados.

15. Quienes participan (mencionar cargos) en el proceso de desarrollo de un nuevo sistema o modificación de uno ya existente.
16. Que documentación es la que acompaña a un sistema cuando se entrega.
17. Se realizan capacitaciones adicionales a la documentación entregada.
18. Se llevan a cabo revisiones para determinar si los sistemas cumplen con los objetivos para los que fueron diseñados.
19. Se lleva a cabo algún tipo de evaluación que verifique el manejo de los sistemas por parte de los nuevos usuarios.
20. Los manuales entregan la información que se adecue a las necesidades de los nuevos usuarios.

ANEXO IV – LISTAS DE CONTROL (CHECK LIST)

Las listas de control, sirven para verificar la existencia de algún control. El tipo utilizado es binario siendo las respuestas alcanzadas, un si o un no.

Las respuestas alcanzadas para cada lista de control fueron obtenidas de las diferentes técnicas utilizadas, como son observación, revisión de documentación, cuestionarios, entrevistas.

Seguridad Física – Oficina de la Sección de Abastecimiento

Preguntas	SI	NO	N/A
1. La oficina cuenta con vigilancia dedicada		X	
2. La oficina cuenta con cámaras de vigilancia		X	
3. Las llaves son administradas por un número reducido y controlado de personas.	X		
4. Cuenta la oficina con extintores		X	
5. Existen políticas de respaldo de información que es manejada por los funcionarios que operan en el área		X	
6. Existe un control de acceso a las dependencias de la oficina		X	
7. Se realiza un control preventivo de los de quipos computacionales en busca de fallas.		X	
8. Existe una persona responsable de la seguridad		X	
9. Existen detectores de humo en el área		X	
10. Existen salidas de emergencia	X		
11. Se prohíbe el consumo de alimentos en el área	X		
12. Se cuenta con copias de seguridad de los archivos en otro lugar de la oficina		X	
13. El lugar donde se ubica el centro de cómputo es seguro contra inundaciones.	X		
14. El lugar donde se ubica el centro de computo es seguro contra incendios.		X	

Seguridad Física en Sala de Servidores

Preguntas	SI	NO	N/A
1. La sala cuenta con vigilancia dedicada		X	
2. La sala cuenta con cámaras de vigilancia		X	
3. El lugar donde se ubica la sala es seguro contra inundaciones.	X		
4. El lugar donde se ubica la sala es seguro contra incendios.		X	
5. Se encuentra la sala debidamente ventilada.	X		
6. La sala de servidores cuenta con detectores de humo.		X	
7. Se realiza mantenimiento al sistema de ventilación de forma permanente.	X		
8. La sala cuenta con acceso restringido.	X		
9. Para acceder a la sala de servidores se debe traspasar 1 o 2 puertas.	X		
10. Las 4 paredes de la sala de servidores son de concreto.	X		
11. La puerta de la sala cuenta con chapa de doble giro.		X	
12. Existen responsables de la seguridad en la sala de servidores		X	
13. Se lleva a cabo un registro de las entradas y salidas del personal que ingresa a la sala de servidores.		X	
14. Ingresa a la sala de servidores personal que no pertenece al área		X	
15. Se registran las actividades realizadas por el personal externo en la sala de servidores.		X	
16. Se prohíbe consumir alimentos y fumar dentro de la sala de servidores.	X		
17. El espacio físico es suficiente para alojar los servidores.		X	
18. Las llaves de los servidores se encuentran guardadas debidamente.		X	
19. Existen seguros comprometidos (Hardware) para cada uno de los servidores.		X	
20. Se utiliza de forma permanente zapatillas para extender el suministro eléctrico hacia los equipos	X		

21. Los servidores o equipos considerados críticos (funcionamiento durante las 24 horas del día), cuenta con UPS independiente.		X	
22. Existe un manual de seguridad para la manipulación del equipamiento.		X	
23. Los rack de los servidores se encuentran anclados a la superficie donde se encuentran emplazados.		X	
24. La sala de servidores cuenta con sensores de humo, humedad.		X	
25. La sala de servidores cuenta con sensores de temperatura.	X		
26. La sala de servidores se encuentra emplaza lejos de lugares de alto tráfico	X.		
27. Los servidores reciben mantenimiento preventivo de forma regular.		X	

Mantenimiento de Equipo Computacional

Preguntas	SI	NO	N/A
1. Se mantiene un inventario del equipamiento computacional existente en el hospital.	X		
2. Se mantiene un inventario del Software instalado en los equipos computacionales.		X	
3. Se mantiene un inventario de las aplicaciones realizadas por terceros o por el personal del hospital.		X	
4. El traslado del equipamiento se realiza mediante una solicitud formal previa.		X	

Protección con Software Malicioso

Preguntas	SI	NO	N/A
1. Todos los equipos computacionales cuenta con un Software antivirus y se actualiza permanentemente.	X		

2. Se mantiene y lista y se controla el acceso a sitios prohibidos para los usuarios (Ej Pornografía)		X	
3. Se dispone de un manual de usuario para la prevención de Software malicioso y para el uso de Software de contención y eliminación.		X	
4. El Software antivirus esta programado para realizar analizar de los equipos automatizados.		X	
5. Se limita la instalación de nuevo Software por parte de los usuarios.	X		

Inscripción e Identificación del usuario

Preguntas	SI	NO	N/A
1. Existe un procedimiento formal para la inscripción y desinscripción de los usuarios de los sistemas.		X	
2. Se mantiene un registro de los usuarios activos del sistema.		X	
3. Existe el procedimiento para asegurar que personal que ya no forma parte de la institución es automáticamente eliminado de los sistemas.		X	
4. Cada usuario es identificado de forma única en los sistemas	X		
5. Existe un procedimiento de control de las actividades de los usuarios en los sistemas.		X	
6. Los sistemas bloquean el acceso ante un ingreso erróneo reiterado.		X	
7. Los sistemas registran los errores que los usuarios cometen	X		
8. Se restringe y controla la asignación y uso de los privilegios.	X		
9. La asignación de claves se realiza mediante un proceso formal.		X	
10. La información almacenada en las bases de datos se encuentra encriptada.		X	
11. Las claves se encuentran encriptadas en las bases de datos, sin		X	

posibilidad de acceso por los administradores.			
12. Las contraseñas tienen una contraseña de un mínimo de 8 caracteres.		X	
13. Existe un procedimiento que impida asignar contraseñas iniciales que se relacionen con datos del usuario.	X		
14. Se cuenta con un procedimiento de cambio de contraseñas permanentes y se controla su ejecución.		X	
15. Existe un procedimiento que impida repetir la misma contraseña al momento de cambiarla.		X	
16. Las contraseñas contienen obligatoriamente caracteres alfanuméricos		X	

Responsabilidades de los Usuarios

Preguntas	SI	NO	N/A
1. Los equipos se bloquean después de un lapso de tiempos inactivos.		X	
2. Se instruye a los usuarios a cerrar sus sesiones cuando no estén activos.		X	

Respaldo de la Información

Preguntas	SI	NO	N/A
1. Existe un cronograma para la rotación y retención de las copias de respaldo.	X		
2. Las copias de seguridad se almacenan en un lugar distinto al centro de cómputos.		X	
3. Los medios de respaldo utilizados son confiables.		X	
4. Se realiza un respaldo diario de la información.	X		
5. Existe un responsable de realizar las copias de seguridad	X		
6. Se rotulan adecuadamente las copias realizadas		X	
7. Se realizan respaldo del Software base utilizada en la		X	

organización.			
8. Se llevan a cabo regularmente pruebas de las copias de información y Software realizadas.		X	
9. Se cuenta con un servicio externo que realice las copias de seguridad.		X	
10. Se han presentado incidentes donde deba hacerse efectivo la restauración de la información a partir de las copias de respaldo.	X		
11. Se registran los procesos de respaldo y recuperación.		X	
12. Las copias se guardan en un lugar lejano del centro de cómputo.		X	
13. Existe un procedimiento formal para dar de baja alguna copia de seguridad.		X	
14. Existe una normativa que le indique a los usuarios que realicen copias de respaldos de la información crítica que manejen.		X	

Documentación

Preguntas	SI	NO	N/A
1. Todos los Sistemas de Información cuentan con documentación.		X	
2. Los sistemas cuentan con documentación actualizada.		X	
3. Los Sistemas de Información considerados como críticos cuentan con manuales de uso, explicativos, detallistas.		X	
4. Se detecta la intención de crear manuales de uso para los usuarios de los Sistemas de Información.		X	
5. Se facilito la entrega de la documentación existente al Equipo Auditor.	X		
6. Se ha instado por parte de la dirección la formulación de manuales de usuario.			X
7. Se cuenta con la documentación de las actualizaciones realizadas a los Sistemas de Información.		X	

Registro de Fallas e incidentes de Seguridad

Preguntas	SI	NO	N/A
1. Se mantiene un registro de las fallas producidas de los sistemas de información.		X	
2. Se mantiene un registro de las fallas producidas por desperfectos en el Hardware.		X	
3. Existe un procedimiento formal para proceder en caso de producirse errores en los sistemas.		X	
4. Existe un procedimiento formal para proceder en caso de producirse errores en el Hardware.	X		
5. Se designan de forma clara los responsables de la seguridad informática.		X	
6. Se mantiene una política de seguridad que abarque a toda la institución.		X	
7. Se evalúa regularmente que las políticas implantadas se lleven a cabo.		X	

Planes de Contingencia

Preguntas	SI	NO	N/A
1. Existe un plan de contingencia en caso de que los Sistemas de Información fallen.	X		
2. Existe un plan de contingencia en caso de que el suministro eléctrico falle.	X		
3. Existe un documento formal que especifique los procedimientos a seguir por el plan de contingencia.		X	
4. Este documento se encuentra plenamente difundido		X	
5. Se realizan simulaciones aplicando el plan de contingencias		X	

Continuidad del Servicio

Preguntas	SI	NO	N/A

1. Se cuenta con un generador de energía eléctrica para la oficina de abastecimiento.		X	
2. Se cuenta con un generador de energía eléctrica para las bodegas.		X	
3. Se cuenta con un generador de energía eléctrica para la sala de servidores.		X	
4. La Sección de Abastecimiento puede continuar operando aún cuando no se cuente con los Sistemas de Información.	X		
5. El personal esta al tanto de cómo proceder en caso de la caída de los Sistemas de Información.	X		
6. Se reingresan todos las órdenes de compra, despacho, recepción recuperados los Sistemas de Información.	X		

Procedimiento de Compras

Preguntas	SI	NO	N/A
1. Las compras son regidas por un programa formal de compras	X		
2. El ingreso de los pedidos es automatizado.		X	
3. Puede anularse las órdenes de compra.	X		
4. Se registran los errores producidos en los procesos de compra	X		
5. El programa de compra es cargado en el Sistema		X	

ANEXO V – METODOLOGIA DE EVALUACION DE RIESGOS

Los procesos relevantes que son llevados a cabo por la Sección de Abastecimiento, el Área de Soporte de Comunicaciones, y la Oficina de Ingeniería de Sistemas se sometieron a la evaluación, teniendo como objetivo detectar la existencia de riesgos y sopesar el impacto que estos producirían a la institución. "Se deben tomar decisiones en relación a que riesgos la organización aceptará y que controles se implementarán para mitigar el riesgo" (Albert, Dorofee, 2003).

El proceso de evaluación de riesgos cuenta con 6 fases, los cuales se ejecutan de forma correlativa:

1. Identificación de Amenazas

Métodos más usados:

- Lluvias de ideas. Riesgos macros hasta micros.
- Segmentar sistema por áreas, por operaciones, por recursos u otros conceptos. Agrupar causas y efectos de un mismo riesgo.
- Redacción en la forma más clara y explícita del posible riesgo.

2. Selección de las Amenazas críticas

Se deben seleccionar las amenazas relevantes para así no afectar a la eficiencia global del sistema con un alto número de controles. Método recomienda un análisis cualitativo de efectos y probabilidad de ocurrencia.

3. Evaluar las implicaciones de costos, eficiencia, etc.

Esta evaluación se realiza si se decide efectuar un control sobre el riesgo.

El propósito de la presente Auditoría es efectuar sugerencias de nuevos controles o medidas, no realizando los análisis de las implicaciones que estas traen consigo.

4. Decisiones de la dirección en cuanto al riesgo.

La administración de la institución decidirá si asume el riesgo o realiza controles.

5. Diseñar Controles

El objetivo es definir los controles para los riesgos críticos identificados. Se recomienda descomponer riesgos en causas, efectos y formas de ocurrencia. Los controles a efectuar deben ser: Prácticos, razonables, costo-efecto, oportunos, significativos, apropiados, simples y operativos.

1.1. Identificación de riesgos

- Daños físicos o destrucción de los recursos
- Pérdida por fraude o desfalco
- Extravío de documentos fuente, archivos o informes
- Robo de dispositivos o medios de almacenamiento
- Interrupción de las operaciones del negocio
- Pérdida de integridad de los datos
- Ineficiencia de operaciones
- Errores

1.2. Tipo de Riesgo – Factor de Riesgo

Una vez identificado los riesgos y amenazas se deberá elaborar una tabla indicando en una columna el tipo de riesgo detectado y en la segunda columna el factor de criticidad asignado (Alto, Medio, Bajo, Muy Bajo). Será de consenso con el auditado los riesgos a ser evaluados y controlados.

Un ejemplo de ellos sería:

Tipo de Amenaza	Factor Criticidad
Robo de Hardware	Alto
Robo de Información	Alto
Efectividad de Controles	Alto
Fallas en los Equipos	Medio
Virus	Medio
Errores	Medio

Accesos no Autorizados	Medio
Discontinuidad Energética	Medio
Robo	Bajo
Fuego	Bajo
Terremotos	Muy Bajo

Tabla 3: Tabla de Amenaza – Factor

2.1 Niveles de Riesgo

Como se muestra en la tabla 3 los riesgos detectados se clasifican por su nivel de importancia, el cual es directamente proporcional a los daños que produce. Para la cuantificación del riesgo de debe asignar un porcentaje a la importancia del riesgo:

- Alto, es igual a 100%
- Medio, es igual al 75%
- Bajo, es igual a 50%
- Muy Bajo, es igual a 25%

Además que cada riesgo detectado y sometido a evaluación debe tener asignado un porcentaje de importancia dentro de la institución, determinado en consenso por el auditado y el Auditor. La suma de los porcentajes de los riesgos deberá ascender al 100%.

Cada riesgo se someterá a evaluación, se comprobará una serie de preguntas, las cuales tendrán un nivel de criticidad:

- Critico (C)
- No Critico (NC)

Cada pregunta tendrá asociada una probabilidad;

- Alta: 1
- Media: 0.75
- Baja: 0.5

La cual indica el porcentaje de que ese control sea vulnerado. Las preguntas podrán poder ser respondidas con:

- 0 para SI
- 2 para NO
- 1 para Parcialmente
- No aplica, dejando en blanco esa evaluación.

La forma de evaluar los riesgos será multiplicar el valor de la probabilidad por la respuesta a la pregunta, la suma de los resultados de cada pregunta se dividirá por la cantidad de respuestas SI, NO, PARCIALMENTE. No se considerarán las preguntas que no se apliquen.

El valor obtenido indicará el nivel de criticidad, pudiendo encontrarse el valor entre el rango:

Resultado	**Riesgo**
0 – 0.25	Prácticamente Nulo
0.26 – 0.75	Poco Importante
0.76 – 1.25	Importante
1.26 – 1.75	Muy Importante
1.76 – 2	Crítico

Tabla 4: Rango de Criticidad

ANEXO VI – ANALISIS DE RIESGOS

1. Análisis de Riesgos

El riesgo es el grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños y / o perjuicios a la Organización[16].

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro.

1.1. Identificación de Amenazas

1.1.1. Accesos no Autorizados

Esta amenaza se hace latente por una falta de medidas o controles efectivos que permitan restringir el acceso a las dependencias sólo a personal autorizado. Dejando expuestos los activos de la organización, sean estos Hardware, información entre otros.

1.1.2. Errores de usuarios, accidentales o intencionados

Esta amenaza se encuentra en toda organización, debiendo plantear medidas que limiten el impacto que su manifestación produzca. Los errores intencionados son los más dañinos ya que se atentará directamente y con el mayor daño posible.

1.1.3. Virus, Malware Informático

La conexión a Internet, la manipulación de dispositivos removibles son una fuente de infecciones permanente que afectan a los Sistemas de Información y a la información que es manipulada por los usuarios. Debiendo ser prevenida con políticas de seguridad establecidas y Software especializado.

16 MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

1.1.4. Deficiente Mantención de los Equipos.

No contar con una mantención planificada permitirá que los errores tanto de Hardware como de Software se presenten con mayor frecuencia. Aumentando el riesgo de pérdida de activos.

1.1.5. Poca Vigilancia

No contar con personal dedicado de seguridad y medios de vigilancia aumenta el riesgo de perdida de productos, equipos, información.

1.1.6. Siniestros

Esta amenaza comprende la presencia de fuego en las dependencias de la organización, sea esta por causas espontáneas o premeditadas, causando daños y pérdidas a la organización. El de perder información, equipos etc. se incrementa si no se han implementado medidas que contribuyan a prevenir o mitigar los daños posibles.

Existen amenazas que pueden redundar en lo mismo como:

- Almacenamiento de Productos Combustibles.
- Falta de Extintores.
- Falta de sensores de Humo.
- Instalaciones Eléctricas deficientes,

1.1.7. Desastres naturales

Las amenazas naturales son inevitables y varían en relación a la zona geográfica donde se encuentra emplazada la institución, algunas de ellas son; Inundaciones, Terremotos, entre otros. De no existir medidas que prevean estas amenazas, el riesgo de pérdida de los activos se eleva considerablemente.

1.1.8. Robos, Mermas de Productos, Activos en General.

Estas amenazas atentan directamente al presupuesto de la institución, y al tratarse de una institución pública como es el caso del HCHM, este es de carácter

limitado, deteriorando el servicio que esta presta a la comunidad. Se deben instaurar medidas que reduzcan la posibilidad de ocurrencia.

1.1.9. Revelación de Información

Amenaza producida por usuarios irresponsables que no resguardan el activo principal de la institución, el exceso de confianza y la falta de controles aumentan el riesgo de develar información confidencial.

Se deben implantar medidas que reduzcan la probabilidad de manifestación de la amenaza, principalmente referido a la seguridad lógica de los Sistemas de Información.

1.1.10. Ataques Externos

Amenaza que afecta a todo Sistema de Información que tenga a acceso a redes externas. Esta amenaza puede atentar contra los Sistemas de Información, denegando los servicios, pérdida o robo de información, entre otros.

1.1.11. Instalación de Software de Terceros

Amenaza permanente producida por una deficiente o nula implantación de políticas de seguridad, con permisos no restrictivos y usuarios no consientes del riesgo que a los Sistemas de Información trae consigo esta práctica. El no conocimiento del Software instalado por parte del Área de Soporte de Comunicaciones aumentan los focos de infecciones, comprometiendo la seguridad.

Pudiendo comprometer los Sistemas de Información, la información manipulada, multas por utilizar Software licenciado.

1.1.12. Uso poco eficiente de los Sistemas de Información

Amenaza producida por una deficiente capacitación de los usuarios, debido una eficiente confección de manuales uso, falta de evaluación de los mismos, poco compromiso de los usuarios, falta de personal. El riesgo de una mala manipulación atenta directamente a la integridad de la información manejada.

Otras amenazas relacionadas son:

- **Satisfacción de los requerimientos actuales,** es importante la actualización de los Sistemas de Información que permitan dar cumplimiento a los requerimientos actuales de la institución.
- **Registro Erróneo de la Información.**

1.1.13. Respaldos y Restauración de Información.

Amenaza producida por una deficiente política de respaldo y restauración de información, que permita asegurar la continuidad de los servicios en caso de producirse algún inconveniente que comprometa la integridad de la información almacenada.

Se acentúa la amenaza al no contar con recursos económicos, humanos y de tiempo.

1.1.14. No disponibilidad de Planes de Contingencia

Todo servicio brindado debe prever que los recursos que lo sostienen pueden fallar debido a diversas causas que escapan de su control. Es por esto que se debe estipular claramente los planes de contingencia que gobiernen las acciones y procesos del personal en caso de no disponer de los Sistemas de Información u otro recurso importante. Garantizando que se dispondrá de los servicios brindados para el bienestar de la organización.

1.1.15. Duplicidad de Procesos

Los Sistemas de Información deben mantenerse interrelacionados y comunicados siempre, evitando que el personal replique información en distintos sistemas. Evitando la perdida de eficiencia y tiempo, reduciendo el riesgo de inconsistencia de la información.

1.1.16. Robo de Información, Fraude, Sabotaje o Interrupción de Servicios.

Amenazas presentes en cada institución que cuente con activos valiosos para alguien. Se debe contar con controles eficientes que eviten en mayor medida la ocurrencia de alguna de estas amenazas, y contar con personal que controle que estas medidas se llevan a cabo.

1.1.17. Compromiso de las bases de Datos

Se deben proteger las bases de datos ante amenazas externas e internas, que intenten acceder a la información almacenada en ellas. Se debe proteger a los usuarios ante ingresos erróneos de información, validando cada ingreso.

Mantener la información encriptada en su almacenamiento y mientras viaja por las diferentes redes utilizadas mitigaran los efectos nocivos de una bases de datos comprometida.

Además se deberá velar por no divulgar información del personal de la institución, como son cuentas de usuario y contraseña

1.1.18. Seguros Comprometidos

La institución debe resguardar y asegurar sus activos críticos con entidades externas que le permitan; Garantizar la continuidad del servicio, disminuir los costos de reposición, reparación de equipamiento, entre otros puntos relevantes.

Lo más importante para una Sección como Abastecimiento es garantizar que el servicio brindado se efectué sin contratiempos, debido a que el riesgo de no contar con el es muy elevado por la naturaleza de la organización.

1.1.19. Deficiente Organización y división de responsabilidades

La Dirección del área y de la organización debe establecer uso eficiente de los recursos con que se cuenta. Velando por un cumplimiento de las obligaciones y una división adecuada de las responsabilidades, poniendo especial énfasis en los procesos críticos del área.

Para ello se deben asignar los recursos mínimos necesarios para un óptimo desempeño.

2. Activos de la Organización

Se denominan activos los recursos del Sistema de Información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema, (datos). Alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (Software) que permiten manejar los datos.
- Los equipos informáticos (Hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

3. Determinación del Riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema.

3.1. Aplicación de la Metodología

ALCANCE : Auditoria a la seguridad Física
ITEMS : Controles de Acceso Servidores
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	**Parcialmente**
N/A	= x	**No Aplica**

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existe acceso restrictivo a los Servidores	B	0,5			2		1		
2	NC	Existe señaletica que restrinja el acceso	B	0,5			2		1		
3	NC	Existen camaras de seguridad en la sala de servidores	B	0,5			2		1	0,833	IMPORTANTE
4	C	La sala donde se ubican, tiene más de una entrada	M	1		0			0		
5	C	Existe un control a la(s) llave(s) de la sala de los servidores p	M	1		0			0		
6	C	Existe un registro de las entradas a la sala de servidores	M	1			2		2		
			Sumatoria			0	8	0	5		

ALCANCE : Auditoria a la seguridad Física
ITEMS : Controles de Acceso a Bodegas
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existe acceso restrictivo a las bodegas	B	0,5			2		1		
2	NC	Existe señaletica que restrinja el acceso	B	0,5		1			0,5		
2	NC	Existe personal de seguridad en bodegas	B	0,5			2		1		
3	C	Existe personal de seguridad fuera de bodegas	M	0,75			2		1,5	0,929	IMPORTANTE
4	NC	Existen camaras de seguridad en cada bodega	B	0,5			2		1		
6	C	Existe un control a la(s) llave(s) de las bodegas	B	0,5		0			0		
7	C	Existe un registro de las entradas a las bodegas	M	0,75			2		1,5		
			Sumatoria			0	10	0	6,5		

ALCANCE : Auditoria a la seguridad Lógica
ITEMS : Registro y Acceso a los Sistemas
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existe método de autentificación del ingreso a los sistemas	A	1		0			0		
2	NC	Se restringue el ingreso erroneo reiterado	A	1			2		2		
2	C	Existe una política de renovación de contraseñas	A	1			2		2		
3	NC	Se restringue la composición de las contraseñas	M	0,75			2		1,5		
4	C	Se registran los errores de los usuarios	M	0,75				1	0,75	1,472	MUY IMPORTAINTE
5	NC	Se solicita el cambio de la contraseña en el 1° ingreso	M	0,75			2		1,5		
6	C	Cada usuario tiene asignado un perfil	A	1		0			0		
7	C	Existe un proceso formal para dar de alta un usuario	A	1			2		2		
8	C	Existe un proceso formal para dar de baja un usuario	A	1			2		2		
9	NC	Los sistemas se bloquean si se mantienen inactivos	M	0,75			2		1,5		
			Sumatoria			0	14	1	13,25		

ALCANCE : Auditoría a los Procesos
ITEMS : Continuidad del Servicio
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	**Parcialmente**
N/A	= x	**No Aplica**

PROBABILIDAD

ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existen procedimientos alternativos en caso de no disponer	A	1		0			0		
2	C	Los procedimiento se encuentran escritos y difundidos	A	1				1	1		
3	C	El personal esta capacitado para operar sin sistemas	M	0,75		0			0	0,625	POCO IMPORTANTE
4	C	Se registran los errores de los usuarios	M	0,75				1	0,75		
5	C	Los servidores cuentan con UPS	A	1				1	1		
6	NC	Cuenta con un suministro de electricidad independiente	B	0,5			2		1		
			Sumatoria			0	2	3	3,75		

ALCANCE : Auditoría a la Seguridad Lógica
ITEMS : Virus, Malware
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Todos los equipos cuenta con software antivirus	A	1		0			0		
2	C	Todos los equipos cuentan con software antimalware	A	1		0			0		
3	C	El software se actualiza automáticamente	A	1		0			0		
4	C	Se restringue el acceso a ciertos sitios peligrosos	A	1		0		1	1		
5	C	Se restringue el uso de dispositivos portatiles	A	1			2		2	0,55	POCO IMPORTANTE
6	NC	Se restingue la instalación de software de terceros	M	0,75				1	0,75		
7	C	El sistema operativo esta estandarizado	M	0,75		0			0		
8	C	El sistema operativo cuenta con los parches de actualizacion	A	1				1	1		
9	NC	Se realizan mantenciones en busca de infecciones	M	0,75				1	0,75		
			Sumatoria			0	2	4	5,5		

ALCANCE : Auditoria a los Procesos
ITEMS : Mantenimiento de Equipamiento
CRITICIDAD: Medio

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Se realizan mantenimientos preventivos a los servidores	A	1			2		2		
2	C	Se realizan mantenimientos preventivos a los equipos de los	A	1			2		2		
3	C	Soporte cuenta con el personal necesario	A	1			2	1	3	1,7	MUY IMPORTANTE
4	NC	Existe un proceso definido en caso de fallas	M	0,75				1	0,75		
5	C	Existen garantias y/o seguros comprometidos	M	0,75				1	0,75		
			Sumatoria			0	6	3	8,5		

ALCANCE : Auditoría a la Seguridad Física
ITEMS : Siniestros Bodegas
CRITICIDAD: Bajo

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD

ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existen extintores proximos a bodegas	A	1		0			0		
2	C	Existen detectores de humo en bodegas	A	1		0			0		
3	C	Existen sensores de temperatura	A	1		0			0	0,125	PRACTICAMENTE NULO
4	C	Los productos infablames se encuentran en un lugar aparte	A	1		0			0		
5	NC	Las salidas se encuentran expeditas	M	0,75				1	0,75		
6	C	Existen mas de una salidad de emergencia	A	1		0			0		
			Sumatoria			0	0	1	0,75		

ALCANCE : Auditoria a la Seguridad Fisica
ITEMS : Siniestros Sala de Servidores
CRITICIDAD: Bajo

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existen extintores proximos a bodegas	A	1			2		2		
2	C	Existen detectores de humo en bodegas	A	1			2		2		
3	C	Existen sensores de temperatura	A	1		0			0	1,125	IMPORTANTE
4	C	Las paredes de la sala son de concreto	M	0,75		0			0		
5	NC	Las salidas se encuentran expeditas	M	0,75				1	0,75		
6	C	Existen mas de una salidad de emergencia	A	1			2		2		
			Sumatoria			0	6	1	6,75		

ALCANCE : Auditoría a la Seguridad Física
ITEMS : Desastres Naturales Servidores
CRITICIDAD: Bajo

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD

ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	La sala de servidores se encuentra sobre la cota 0	A	1		0			0		
2	C	Existen seguros comprometidos en caso de perdidas	A	1				1	1		
3	C	El edificio es antisismico	A	1		0			0		
4	NC	Se cuenta con sensores de humedad	B	0,5			2		1	0,5	POCO IMPORTANTE
5	C	Se cuenta con respaldos de la información	A	1		0			0		
6	NC	Los servidores se encuentran fijados a la pared o suelo	M	0,75			2		1,5		
7	C	Se cuenta con respaldos de los sistemas	A	1		0			0		
			Sumatoria			0	4	1	3,5		

ALCANCE : Auditoría a la Seguridad Lógica
ITEMS : Integridad de Datos
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

Nº	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Los datos en el sistema base estan encriptados	A	1			2		2		
2	C	Los datos en la red viajan encriptados	A	1			2		2		
3	C	La información personal se encuentra encriptada	A	1			2		2		
4	C	Se restringue el acceso a los sistema	A	1		0			0	1,143	IMPORTANTE
5	C	Se registran las acciones de los usuarios	A	1		0			0		
6	C	Se encuentran bien limitados los perfiles de los sistemas	A	1				1	1		
7	C	Se verifica que la informacion de los sistemas concuerde con	A	1				1	1		
			Sumatoria			0	6	2	8		

ALCANCE : Auditoría a la Seguridad Lógica
ITEMS : Ataques Externos
CRITICIDAD: Bajo

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Los sistemas de informacion cuentan con un firewall	A	1		0			0	0,25	PRACTICAMENTE NULO
2	NC	se registran los ataques producidos	M	0,75				1	0,75		
3	C	Los sistemas cuentan con software contra malware	A	1		0			0		
			Sumatoria				0	1	0,75		

ALCANCE : Auditoría a los Procesos
ITEMS : Capacitaciones
CRITICIDAD: Medio

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Se realizan capacitaciones formales al personal nuevo	A	1			2		2		
2	C	Se realizan capacitaciones formales de los sistemas nuevos	A	1				1	1		
3	C	El área cuenta con un manual de uso especializado	A	1			2		2	1,083	IMPORTANTE
4	C	Se controla que el uso de los sistemas sea el indicado	M	0,75				1	0,75		
5	NC	Existen un responsable de controlar la buena utilizacion de l	M	0,75				1	0,75		
6	NC	El personal sabe a quien acudir en caso de dudas	M	0,75		0			0		
			Sumatoria			0	4	3	6,5		

ALCANCE : Auditoría a los Procesos
ITEMS : Actualización de los Sistemas
CRITICIDAD: Medio

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD

ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Los sistemas satisfacen los requerimientos actuales	A	1				1	1		
2	C	Se genera la instancia de plantear nuevas sugerencias	M	0,75				1	0,75		
3	C	El personal participa en la captura de requerimientos de las r	M	0,75				1	0,75	0,875	IMPORTANTE
4	C	Se cuenta con un captura automatizada de productos	A	1			2		2		
5	NC	Existen un responsable de controlar la buena utilizacion de l	M	0,75				1	0,75		
6	NC	El personal sabe a quien acudir en caso de dudas	M	0,75		0			0		
			Sumatoria			0	2	4	5,25		

ALCANCE : Auditoria a los Procesos
ITEMS : Respaldos y Restauración
CRITICIDAD: Alto

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD

ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD

C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existen politicas definidas de respaldo de información	A	1				1	1		
2	C	Existen politicas definidas de restaurancion de información	A	1				1	1		
3	C	Existe un responsable de las copias de seguridad	A	1		0			0		
4	C	Se almacenan en un lugar externo a la oficina	M	0,75			2		1,5	0,964	IMPORTANTE
5	NC	Se rotulan debidamente las copias de respaldo	M	0,75			2		1,5		
6	NC	Se realizan mantenciones a preventivas a los equipos de res	M	0,75				1	0,75		
7	C	Existe un procedimiento en caso de fallar la restauración	A	1				1	1		
			Sumatoria			0	4	4	6,75		

ALCANCE : Auditoria a los Procesos
ITEMS : Organización y Distribución de Responsabilidades - Abastecimiento
CRITICIDAD: Medio

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existe responsables de la seguridad en la sección de abaste	A	1				1	1	0,333	Poco Importante
2	C	Existen subrogantes para los cargos principales	A	0,75		0			0		
3	C	Los subrogantes tienen las mismas atribuciones	A	0,75		0			0		
			Sumatoria			0	0	1	1		

ALCANCE : Auditoria a los Procesos
ITEMS : Organización y Distribución de Responsabilidades - Soporte de Comunicaciones
CRITICIDAD: Medio

Cuando las respuestas sean:

SI	= 0	
NO	= 2	
PA	= 1	Parcialmente
N/A	= x	No Aplica

PROBABILIDAD	
ALTA	1
MEDIA	0,75
BAJA	0,5

FACTOR DE CRITICIDAD	
C	Critico
NC	No Critico

N°	CRITICIDAD	PREGUNTA	PROB.	PROB.	N/A	SI	NO	PA	RES.	RIESGO	RIESGO
1	C	Existe responsables de la seguridad en la sección de abaste	A	1				1	1	0,75	Poco Importante
2	C	Existen subrogantes para los cargos principales	M	0,75		0			0		
3	C	Los subrogantes tienen las mismas atribuciones	M	0,75		0			0		
4	C	Existe el personal suficiente para las labores	A	1			2		2		
			Sumatoria			0	2	1	3		

4. Contramedidas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

ANEXO VII – Estados de Pedidos

Definición Estados de pedidos.

Existen siete estados para las licitaciones que se procesan en el Sistema ANITA, las que se detallaran a continuación:

Estado 1: Generado mientras se realiza el ingreso de datos a la licitación en Sistema ANITA.

Estado 2: La licitación adquiere este estado cuando es confirmada por el ejecutivo de Compras y es enviada vía Sistema ANITA al departamento de Contabilidad para su aprobación presupuestaria.

Estado 3: Se adquiere este estado cuando la licitación obtiene la aprobación presupuestaria.

Estado 4: Una vez que la licitación cuenta con la aprobación, es replicada en el sistema del portal Mercado Público adquiriendo el estado 4.

Estado 5: Cuando concluye el proceso de licitación y es el pedido es recepcionado por la Sección de Abastecimiento, se adquiere el estado 5.

Adicionalmente existen 2 estados que reflejan errores en el proceso de licitación como son el estado 6 y estado 7, los cuales se explican a continuación:

Estado 6: Corresponde a aquellas licitaciones que presentan errores en sus fase inicial, por parte del ejecutivo de compras, esta licitación errónea debe ser revisada por departamento de Contabilidad, para ser dada de baja y reingresar la licitación en forma correcta.

Estado 7: Este estado es una variante del estado 5 utilizado para reflejar que el pedido presento diferencias entre lo licitado y lo recepciona do.