AUDITORÍA INFORMÁTICA A NIVEL DE LOS SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO

JHOANA LORENA HERNÁNDEZ BENAVIDES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2014

AUDITORÍA INFORMÁTICA A NIVEL DE LOS SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO

JHOANA LORENA HERNÁNDEZ BENAVIDES

Trabajo de grado presentado como requisito parcial para optar el título de Ingeniera de Sistemas

Asesor:
Manuel Bolaños Gonzales
Ingeniero de Sistemas

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2014

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Concejo Directivo de la Universidad de Nariño.

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

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

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____
Presidente de tesis

_____
Jurado

_____
Jurado

San Juan de Pasto, 2014

AGRADECIMIENTOS

Gracias Dios por acompañarme y guiarme a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobretodo felicidad.

A mis padres; Floresmilo Hernández, porque siempre me ha brindado su fuerza y apoyo; a mi madre Corona Benavides por sus enseñanzas y su amor, y aunque no esté presente, vive en mi corazón y desde el cielo me acompaña.

A mis hermanos Yexon y Henry, por ser parte importante de mi vida y representar la unidad familiar, la confianza y la gratitud, porque dia a dia han llenando mi vida de amor y alegrías.

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

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

Al Ingeniero Vicente Chamorro, por ser más que un maestro y dedicarme su tiempo, para guiarme tanto en mi trabajo de tesis como en la vida.

A Andrés Buesaco, por sus palabras de ánimo, por su paciencia y su incondicionalidad.

.

DEDICATORIA

A Dios.
Por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los Momentos difíciles que me han enseñado a valorar cada día.

A ti Madre.
Por la educación recibida, por corregir mis errores y por sus grandes consejos, por el amor que
siempre me has brindado, por cultivar e inculcar ese sabio don de la responsabilidad.
¡Gracias por darme la vida!

A ti Padre.
A quien le debo todo en la vida, le agradezco el cariño, la comprensión, la paciencia y el
apoyo brindado en el transcurso de mi vida y mi carrera profesional.

A mis Hermanos
Por que siempre he contado con ellos para todo, gracias a la confianza que siempre nos
hemos tenido; por el apoyo y amistad

¡Los Amo!

¡Gracias!

RESUMEN

La Auditoría Informática se encarga de verificar el correcto funcionamiento de los equipos computacionales, así como analizar el software legal e ilegal que posee la empresa para así evitar problemas en el ámbito legal y de esta manera solicitar la adquisición de licencias o caso contrario proceder a la desinstalación del mismo, de la misma forma identificar el software que no es necesario para cumplir con el trabajo según el cargo que se tenga.

Estos y otros puntos como el inventario de hardware, componentes lógicos y software se tomaron en cuenta para el desarrollo del presente proyecto, que proporcionará las conclusiones y recomendaciones finales en base al punto de vista informático.

La Empresa DISPROPAN S.A.S ha venido careciendo de un manual de Auditoría Informática, el cual contenga toda la información en el ámbito informático de las Secciones Contabilidad, Bodega, Tesorería, Agencias Norte, Sur y Dirección Financiera.

Cabe mencionar que dicha auditoría se puede realizar tantas veces el cliente lo requiera y de esta manera evaluar la eficiencia de cada una de las áreas, para beneficiar tanto a la empresa, a sus departamentos y a los usuarios que de una u otra forma requieren el servicio de la entidad.

Gracias al presente proyecto investigativo se logró tener un mejor control en el ámbito informático de las diferentes áreas.

ABSTRACT

Computer Audit is responsible for verifying the correct operation of computer equipment and to analyze the legal and illegal software company has to avoid problems in the legal field and thus apply for license acquisition proceed to uninstall it, just as identify software is not needed to accomplish the work according to the position you have.

These and other points as the logical hardware inventory and software components were taken into account in the development of this project, which will provide the final conclusions and recommendations of computer view point.

The Company DISPROPAN SAS has been lacking a Computer Audit Manual, which contains all the information in the information field of Accounting, Industrial, Treasury, Agencies North, South and Financial Management Sections.

It is that such audit can be performed many times the client requires and thus evaluate the efficiency of each of the areas to benefit both the company, its departments and users that require one form or another service of the entity.

Thanks, this research project will be achieved better control in the computer field in different areas.

CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

LISTADO DE IMAGENES

Pág.

GLOSARIO

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

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

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

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

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

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables,

rol claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

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

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

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

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

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

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

TI: Tecnologías de Información

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

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

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

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

Syscafé S.A: Es una empresa líder en el desarrollo de software de gestión comercial, proveedor de servicios de sistematización, que aplica estándares de calidad en sus productos y los adapta a las necesidades del cliente.

INTRODUCCION

En la actualidad es de vital importancia la presencia de las herramientas informáticas para realización de tareas, la optimización de procesos, por esta razón el proveer a cualquier empresa de tecnología es hoy en día una necesidad primordial, puesto que la sistematización trae como resultado la mejora del cumplimiento de los objetivos empresariales y es por ello que de la capacidad de adaptación de la empresa a los cambios dependerán no solo los beneficios sino también su existencia como empresa. Pero un punto fundamental que deben tener en cuenta las organizaciones o empresas, es la supervivencia en caso de pérdidas catastróficas provocadas por accidentes, negligencias, falta de profesionalismo o cualquier otro causal de pérdida o efecto dañoso que amenace con interrumpir las operaciones de la organización, para su crecimiento o reducir sus utilidades.la Auditoría consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades por tal motivo se hace necesario definir métodos y controles que ayuden a estimar la magnitud del manejo de cada área o de cada proceso que se lleve dentro de la empresa como tal.

Lo anteriormente mencionado lo aplica la Auditoría con el objetivo de proporcionar análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas a través de la aplicación de diferentes técnicas que garanticen la confidencialidad, integridad y disponibilidad de la información de todos los procesos que formen parte de la empresa.

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permiten dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

DISPROPAN S.A.S. es una empresa dedicada a la distribución y comercialización de productos e insumos para el sector Panadero, Pastelero y de Alimentos en los departamentos de Nariño y Putumayo. Ofreciendo un amplio portafolio de productos garantizando calidad, servicio y confiabilidad a los clientes, contribuyendo con el desarrollo de la región y compromiso con el medio ambiente. Enfocando sus objetivos al mejoramiento de todos los procesos, entre ellos la administración de los sistemas operativos con el objetivo de garantizar la continuidad y el funcionamiento de las máquinas y del software al máximo rendimiento.

Sabiendo que la razón más importante de una organización es la información, por ende los recursos tecnológicos que se utilizan ya que en ellos se registra y se procesa la información, no se debe olvidar que también son susceptibles de

amenazas, motivo por el cual se ve la necesidad de tener planes y políticas para la protección de estos recursos, por tal razón se presenta el trabajo de grado **AUDITORÍA INFORMÁTICA A NIVEL DE LOS SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO** el cual corresponde a la modalidad de trabajo de aplicación bajo la línea de investigación de Sistemas Computacionales.

La aplicación de la auditoría va orientada a evaluar el Hardware de los equipos de cómputo, dispositivos móviles y redes, en cuanto a su funcionamiento, actualización y mantenimiento, el software instalado en los equipos, el sistema de información de SYSCAFE y su debido contrato de servicios, lo cual permitirá obtener un diagnóstico para así definir planes de mejoramiento para la integración de la tecnología a los procesos de la organización.

IDENTIFICACION DEL PROBLEMA

Título del proyecto:

AUDITORÍA INFORMÁTICA Y DE SISTEMAS APLICADA EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO

TEMA

Auditoría aplicada al área de sistemas, en la parte de hardware e indicadores de funcionamiento de la Empresa Dispropan S.A.S de Nariño y Putumayo

MODALIDAD

Este trabajo de grado, corresponde a la modalidad de TRABAJO DE APLICACION, a realizarse en la EMPRESA DISPROPAN S.A.S. de Nariño y Putumayo. Trabajo que permitirá acrecentar conocimiento y generar diferentes alternativas de desarrollo empresarial por medio de la aplicación de métodos organizacionales, de funcionamiento, aplicación y cumplimiento de políticas, leyes y normas, necesarias para el funcionamiento de una empresa.

LINEA DE INVESTIGACION

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

DEFINICION DEL PROBLEMA

Planteamiento del problema:

La Información es un recurso vital, producido por los sistemas de información. Las organizaciones utilizan también otros recursos como materiales, materias primas, energía y recursos humanos, todos ellos sujetos cada vez a mayores restricciones en su uso y crecimiento, debido a problemas de escasez y, por tanto de costo.
Debe considerarse que un sistema de información no tiene porqué ser asociado a los sistemas informáticos, con los que muchas veces se les confunde. Por el contrario, un sistema de información puede ser una persona, un departamento, toda la empresa. El Sistema de Información comprende, la planificación, recursos humanos y materiales, objetivos concretos a corto, medio y largo plazo, aunque también tecnología y técnicas.

Con los adelantos tecnológicos actuales, sobre todo en las tecnologías de información, es casi imposible que una empresa no haga uso de la información para el desarrollo de sus actividades cotidianas; tan solo tener la información adecuada de un estado financiero no necesariamente en computadoras demuestra que es necesaria la información para todo tipo de actividades y si a esto se le agrega el uso de computadoras como herramientas junto con sistemas capaces de ofrecer la información en forma rápida, ordenada, y concreta, además que el Internet se ha vuelto tan importante y popular para cualquier tipo de persona como para cualquier tipo de empresa sabiendo de antemano que la información es vital en todos los aspectos, muchas empresas emplean Internet como medio de información con sus posibles consumidores, proveedores, socios, siendo este el caso de la empresa en mención permitiéndole de esta manera tener un alto nivel de competitividad y posibilidades de desarrollo.

Con el objetivo de obtener un diagnóstico para definir planes de mejoramiento para la integración de la tecnología a los procesos de la empresa surge la necesidad de desarrollar la auditoría **AUDITORÍA INFORMÁTICA Y DE SISTEMAS APLICADA EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO** la cual evaluará su eficiencia y eficacia.

Formulación del problema

¿Cómo la evaluación de la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, los servidores y el funcionamiento del sistema SYSCAFE ayudarán a definir y establecer un plan de mejoramiento para en la empresa DISPROPAN S.A.S.?

Sistematización del problema

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

- ¿Cómo identificar falencias y puntos críticos en la parte de hardware de equipos de cómputo, en cuanto al sistema de información SYSCAFE, contratos y soporte?

- ¿Cómo garantizar el correcto funcionamiento del Hardware de cómputo, procesos e información de la empresa DISPROPAN S.A.S.?

OBJETIVOS

Objetivo general

Realizar una auditoría que permita evaluar la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, los servidores y el funcionamiento del sistema SYSCAFE para en la empresa DISPROPAN S.A.S, aplicando los procesos de análisis de riesgos y auditoría teniendo en cuenta el modelo estándar de auditoría y mejores prácticas COBIT como herramienta de apoyo en el proceso evaluación de los riesgos existentes y verificación de cumplimiento de controles, con el propósito de ayudar a definir y establecer un plan de mejoramiento e integración de tecnología.

Objetivos específicos

Realizar una evaluación mediante las prácticas de auditoría para identificar los posibles puntos críticos dentro de los procesos del hardware, en cuanto a servidores, equipos de cómputo e indicadores de funcionamiento real de la empresa.

Realizar una evaluación de los puntos críticos e identificar falencias en la parte de hardware de equipos de cómputo, en cuanto al sistema de información SYSCAFE, contratos y soporte, mediante las prácticas de auditoría.

Realizar una evaluación mediante las prácticas de auditoría para garantizar el correcto funcionamiento del Hardware de cómputo, procesos e información de la empresa DISPROPAN S.A.S

JUSTIFICACIÓN

En la actualidad la empresa DISPROPAN ve la necesidad de realizar un mejoramiento de los desarrollos y procesos llevados a cabo en la empresa para lo cual se desarrollará un diagnostico a todos los procesos de información que se desarrollan en la empresa cede principal y dentro de sus agencias, puesto que la empresa ha tenido un crecimiento en los últimos años, y para lo anterior se hace necesario realizar una auditoría interna para lograr los resultados esperados.

Dentro de la auditoría a realizar se han tomado los procesos de mejoramiento de Hardware y Software de información, Hardware y Software de redes actualización y cambio del sistema de información de SYSCAFE y contratación, desde la sede principal como también las diferentes agencias a su cargo la cual se centrara el proceso de auditoría.

Para los procesos mencionados y teniendo en cuenta las nuevas exigencias del Control Interno y los modelos de Control existentes tales como COSO, COCO, etc., se plantea el empleo de un nuevo modelo llamado COBIT cuyas siglas significan: Objetivos de Control para la Información y Tecnologías afines.

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

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

ALCANCE Y DELIMITACIÓN

La presente auditoría pretende evaluar las condiciones actuales del Hardware de los equipos, Hardware de las redes y servicio de red, el Software, el Sistema Informático y su funcionalidad dentro de la empresa DISPROPAN, con el fin de observar las fallas posibles en su conjunto, verificar el cumplimiento de normas y así optimizar el uso de los recursos para brindar un buen servicio a los usuarios de la empresa.

En razón de lo anterior es importante Conocer que DISPROPAN cubre los departamentos de Putumayo y Nariño, por lo tanto el trabajo se aplico a la sede principal como también a sus agencias clasificadas así:

- Central Pasto
- Ipiales
- Tumaco
- Mocoa
- Puerto Asís

Los puntos a evaluados son los siguientes:

- PROCEDIMIENTO DE LAS ACTIVIDADES DEL PERSONAL: Conocer los procesos de cada trabajador, los equipos necesarios y/o herramientas que necesitan para realizar su trabajo eficientemente.
- VERIFICAR LA EXISTENCIA DE UN MANUAL DE FUNCIONES: confirmar que se cumplan las funciones establecidas dentro del manual y que se respeten los cargos jerárquicos dentro del organigrama.
- VERIFICAR LA CONFIGURACION DE LOS EQUIPOS: se evaluara si la configuración con la que trabajan los equipos es la adecuada y cumple con las especificaciones técnicas y es acorde a los procesos realizados.
- SERVIDORES Y EQUIPOS DE COMPUTO: revisar garantías, instalaciones, respaldos, planes de contingencia, políticas de seguridad, política de mantenimiento con sus respectivos formatos de registro e instructivos.

Con lo anterior se logró que la empresa desarrolle planes de mejoramiento que le permita tomar medidas de seguridad y control de todo el Sistema Informático

1. MARCO TEORICO

1.1 ANTECEDENTES

Uno de los avances más importante de los últimos años es la tecnología y con ello el cambio drástico que el mundo ha tenido con el paso del tiempo, el competitivo campo laboral ha adaptado de forma muy positiva el manejo de la tecnología.

Teniendo como resultado que la información de una empresa este bien organizada, de esta manera se hace necesario tener un control de las herramientas como equipos de cómputo, equipos de comunicación, bases de datos, redes y sistemas de información, para saber así con que herramientas se cuenta y que tan actualizados están, lo anterior combinado con la necesidad de obtener un plan estratégico y corporativo que le permita a la empresa conocer las fortalezas y debilidades que genere a la parte administrativa seguridad, confiabilidad, efectividad y eficacia de su entorno, a partir de esto se hace necesario que se lleve a cabo una auditoría de acuerdo con las necesidades que existan en la empresa.

En la actualidad la empresa DISPROPAN ve la necesidad de realizar un mejoramiento de los desarrollos y procesos llevados a cabo en la empresa para lo cual se desarrollará un diagnóstico a todos los procesos de información que se desarrollan en la empresa cede principal y dentro de sus agencias, puesto que la empresa ha tenido un crecimiento en los últimos años, y para lo anterior se hace necesario realizar una auditoría interna para lograr los resultados esperados.

Dentro de la auditoría se toman los procesos para mejoramiento de Hardware y Software de información, Hardware y Software de redes, actualización o cambios del sistema de información de SYSCAFE y el proceso de contratación del sistema de información SYSCAFE, tanto para la sede principal como también las diferentes agencias a su cargo.

La auditoría se hace necesaria para la integración de tecnología a los procesos de manejo de la información, ya que hasta el momento no se ha realizado ningún tipo de evaluación ni en los procesos, ni en el uso de los recursos informáticos que están actualmente en funcionamiento dentro de la organización.

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

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

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

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

1.2 ASPECTOS GENERALES DE LA AUDITORÍA

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

Por lo general el área de sistemas de una empresa, es un espacio dotado de recursos tecnológicos como equipos de cómputo, impresoras, equipos de comunicaciones, donde prácticamente se realiza todo el procesamiento de la información, que por razones de organización se hace necesaria la auditoría[1]. Existen algunas funciones del área de sistemas, que son:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2.3 Funciones principales:

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

- Ejercer revisión en forma preventiva a los egresos ejecutados por la empresa.
- Evaluar los procesos informáticos de la empresa.

1.2.4 Clasificación de la auditoría:

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

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

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

1.2.5 Tipos de auditoría:

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

el Código de Comercio, Código Orgánico Tributario, y demás leyes impositivas que corresponda aplicar.

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

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

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

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

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

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

Auditoría informática: La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

1.3 AUDITORÍA INFORMÁTICA COMO OBJETO DE ESTUDIO

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

Los factores que pueden influir en una organización a través del control y la auditoría en informática, son:

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

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

1.3.1 Objetivo fundamental de la auditoría informática. La operatividad en una empresa es el punto más importante, es la encargada de vigilar el funcionamiento

de mínimos consistentes de la organización y las máquinas a nivel global como parcial. La auditoría se debe realizar en el momento en que la maquinaria informática está en funcionamiento, con el fin de identificar falencias que obstruyan la operatividad de las mismas, con el objeto de corregir o buscar alternativas de solución a tiempo, sin tener que parar el trabajo.

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

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

Los Controles Técnicos Específicos, menos evidentes, son también necesarios para lograr la operatividad de los sistemas. Es decir por más pequeña que sea la aplicación que se deba ejecutar, esta debe funcionar al máximo, evitando así la inoperatividad, bien sea en hardware como en software. Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observación de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

- Las Normas Generales de la Instalación Informática. Se realiza una revisión inicial sencilla, verificando la aplicación de las normas pero también registrando las áreas que no cumplan o que no las apliquen, sin olvidar que esta normativa no está en contradicción con alguna norma no informática de la empresa.
- Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por la persona responsable de este cargo.

Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

- Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

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

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la Auditoría de Seguridad Informática en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática.

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

Teniendo en cuenta lo anterior y partiendo de las diferentes actividades de sistemas que cada empresa tiene dentro de su organización dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Áreas Específicas de la Auditoría Informática más importantes. Cada área específica puede ser auditada desde los siguientes criterios generales, que pueden modificarse según sea el tipo de empresa a auditar:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.

- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

1.3.3 CLASIFICACIÓN DE LA AUDITORÍA INFORMÁTICA

Auditoría informática de explotación: Explotación Informática se encarga de obtener resultados informáticos, como son: listados impresos, ficheros soportados magnéticamente, órdenes automatizadas para lanzar o modificar procesos industriales, entre otras. Los datos es la materia prima que hay que transformar por medio del proceso informático (gobernado por programas), bajo el criterio de integridad y control de calidad y así lleguen finalmente al usuario. Para auditar explotación hay que auditar las sesiones que la componen y sus interrelaciones.

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

- **Sistemas operativos:** Debe verificarse en primer lugar que los Sistemas estén actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas.
- **Software básico:** Es fundamental para el auditor conocer los productos de software básico que han sido adquiridos aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.
- **Tunning:** Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados.
- **Optimización de los sistemas y subsistemas:** Las Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings pre-programados o específicos. El auditor verificará

que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

- **Administración de base de datos:** El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. El auditor de Base de Datos analizará los Sistemas de salvaguarda existentes, revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.
- **Investigación y desarrollo:** Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del mismo campo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas. La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas

Auditoría informática de comunicaciones y redes: Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios). El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de

Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

Auditoría informática de desarrollo de proyectos o aplicaciones: El Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones, que a su vez, engloba muchas áreas que tiene la empresa. Una Aplicación recorre las siguientes fases:

- Pre-requisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (pre-programación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

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

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

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

1.3.4 Metodología de auditoría informática. Como auditor se debe recolectar toda la información general, que permita así mismo definir un juicio global objetivo siempre amparadas en pruebas o hechos demostrables. Dar como resultado un informe claro, conciso y a la vez preciso depende del análisis y experiencia del auditor, frente a diferentes entornos a evaluar, dependiendo de las debilidades y

fortalezas encontradas en dicha empresa auditada. La recolección de información, el análisis, la aplicación de diferentes normas de acuerdo al tipo de auditoría, los hallazgos encontrados y pruebas que avalen estos resultados son indispensables en la realización de una auditoría. Para llegar al resultado hay que seguir una serie de pasos que permiten tener claridad y orden de la auditoría aplicar.

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

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

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

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

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

- Organigrama: El organigrama expresa la estructura oficial de la organización a auditar. Permite identificar las jerarquías, dependencias y direcciones entre las áreas existentes.
- Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.
- Relaciones Jerárquicas y funcionales entre órganos de la Organización: El auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de Jerarquía implican la correspondiente

subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

- Flujos de Información: Además de las corrientes verticales intra - departamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra-departamentales.
- Número de Puestos de trabajo: El equipo auditor comprobará que los nombres de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.
- Número de personas por Puesto de Trabajo: Es un parámetro que los auditores informáticos deben tener en cuenta ya que la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.
- Entorno operacional: El auditor informático debe tener una referencia del entorno en el que va a desenvolverse y se obtiene determinando lo siguiente:
- Situación geográfica de los Sistemas: Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa, continuando con la verificación de la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.
- Arquitectura y configuración de Hardware y Software: Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, para esto es importante que los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.
- Inventario de Hardware y Software: El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPU‟S, unidades de control local y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
- Comunicación y Redes de Comunicación: Al realizar el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, igualmente, poseerán información de las Redes Locales de la Empresa y todo lo que tenga que ver con la red de Comunicaciones.

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

Recursos humanos: La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es igualmente señalable que la auditoría en general suele ser ejercida

por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria. Recursos materiales: Los recursos materiales del auditor son de dos tipos:

- Recursos software como son, Cantidad y complejidad de Bases de Datos y Ficheros, que son programas propios de la auditoría, son muy potentes y Flexibles.
- Recursos materiales Hardware: Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado. Por lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, scanner, etc.

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

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

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

Actividades propiamente dichas de la auditoría Informática: La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor

calidad. Existen técnicas que hacen que el auditor las aplique de acuerdo a su juicio y al tipo de auditoría a ejecutar y son:
Técnicas de Trabajo:

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

Herramientas:

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

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

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

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

- Tendrá como máximo 4 folios
- Incluirá fecha, naturaleza, objetivos y alcance
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

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

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

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

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

Modelo conceptual de la exposición del informe final:

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

    - El hecho debe poder ser sometido a cambios.
    - Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
    - No deben existir alternativas viables que superen al cambio propuesto.

- La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación.

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

Flujo del hecho o debilidad:
Hecho encontrado.

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

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

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

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

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

1.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA[4]

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

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

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre-impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

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

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

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

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

1.4.3 Checklist. El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al

auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

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

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma. Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable.

El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer. Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

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

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

imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

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

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

- Muy deficiente.
- Deficiente.
- Mejorable.
- Aceptable.
- Correcto.

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

- ¿Existe personal específico de vigilancia externa al edificio?

Rta/ No, solamente un guarda por la noche que atiende además otra instalación adyacente.
<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?

Rta/ Si, pero sube a las otras 4 plantas cuando se le necesita.
<Puntuación: 2>

- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

Rta/ Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
<Puntuación: 2>

- El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

Rta/ No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.
<Puntuación: 4>

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

Checklist Binaria: Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente. Ejemplo:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

- ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

- ¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

- ¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

- ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

- ¿Se conoce la norma anterior?

<Puntuación: 0>

- ¿Se aplica en todos los casos?

<Puntuación: 0>

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor. Las Checklists Binarias siguen una elaboración inicial mucho más

ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo. No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

1.4.4 Trazas y/o huellas. Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo. Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

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

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

- Observación histórica, entre las cuales están:
    - Observación controlada
    - Observación natural

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

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

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

1.5 ESTANDARES DE AUDITORÍA

Para la realización y ejecución de una auditoría se hace necesario aplicar normas o estándares bajo los cuales las empresas deben regirse, de allí la importancia identificar los estándares internacionales que en este caso son:[5]

Directrices Gerenciales de COBIT, desarrollado por la Information Systems Audit and Control Association (ISACA) Asociación de Auditoría y Control de los Sistemas de Información: Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y administre los riesgos relacionados con la tecnología de información y establezca

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

el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados. Uno de los objetivos de ISACA es promover estándares aplicables internacionalmente para cumplir con su visión. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoría, como:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor, CISA) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias, así:

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

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

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

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA: Este servicio pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la

confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

Modelo de Evolución de Capacidades de software (CMM), desarrollado por el Instituto de Ingeniería de Software (SEI): Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización, con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

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

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

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

Administración de seguridad de información: Aprendiendo de organizaciones líderes, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO): Este modelo considera ocho organizaciones privadas reconocidas como líderes respecto a seguridad en cómputo. Este trabajo hace posible la identificación de 16 prácticas necesarias para asegurar una adecuada administración de la seguridad de cómputo, las cuáles deben ser suficientes para

incrementar significativamente el nivel de administración de seguridad en tecnología de información y comunicación electrónica.

1.5.1 El Modelo COBIT para auditoría y control de sistemas de información[6]. La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. Las siglas COBIT significan Objetivos de Control para Tecnología de Información (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association). COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización. “La adecuada implementación de COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado. Cualquier tipo de empresa puede adoptar una metodología COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos IT y consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos”, Señaló un informe de ETEK. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

1.5.2 Criterios de información de COBIT. Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales

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

son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

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

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

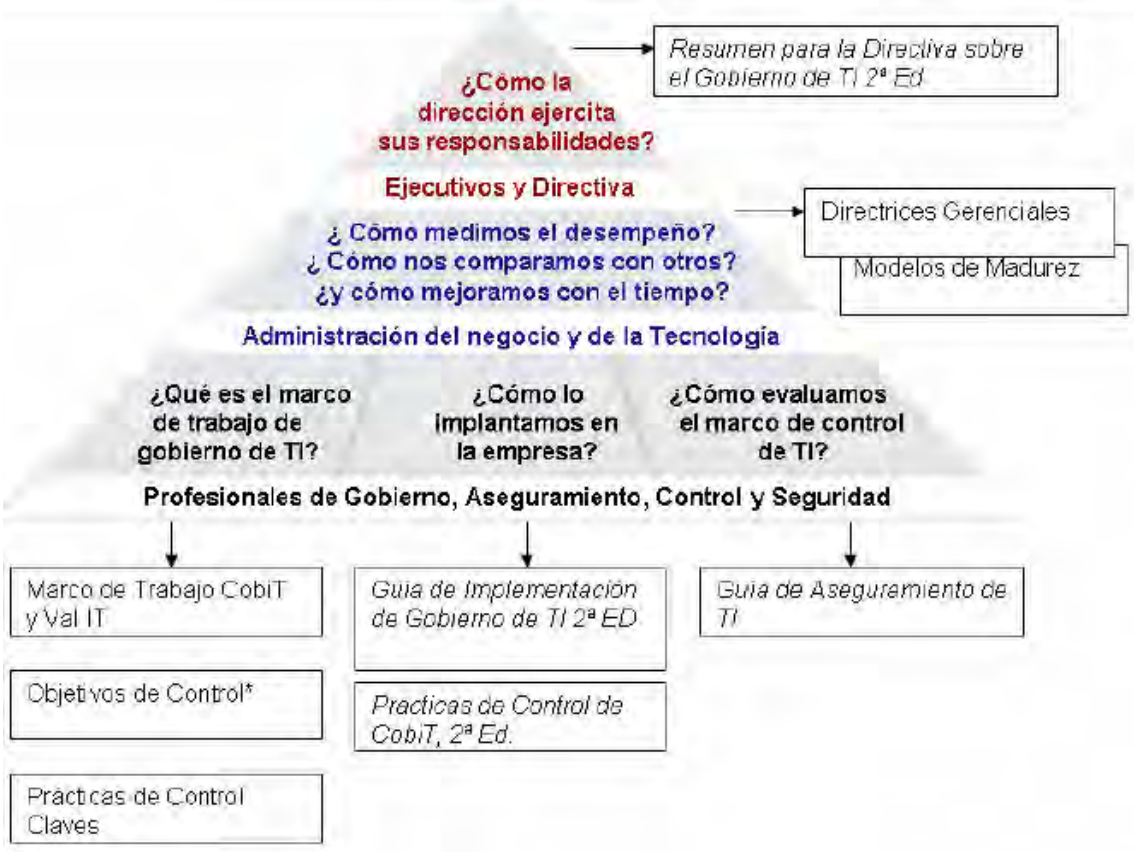
- La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a lo siguiente[7]:

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

[7] http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

Figura 1. Diagrama de contenido del COBIT[8]



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

Brevemente, los productos COBIT incluyen:

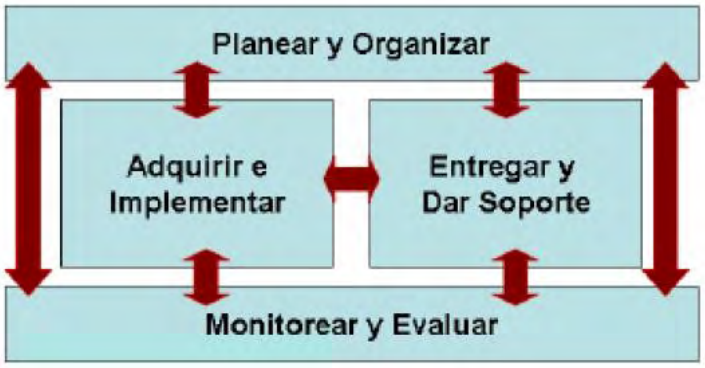
- **El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición:** Diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.
- **Directrices gerenciales / modelos de madurez:** Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad. Marco de Referencia: Explica cómo COBIT

[8] http://cs.uns.edu.ar/~ece/auditoria/COBIT-CURNE-UASD

organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.

- **Objetivos de control:** Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todas los procesos de TI
- **Guía de implementación de gobierno de TI:** Usando COBIT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI.
- **Prácticas de control de COBIT:** Guía para Conseguir los Objetivos de Control para el Éxito del Gobierno de TI 2ª Edición: Proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos.
- **Guía de aseguramiento de TI:** Usando COBIT: Proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control. El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

Figura 2. Cuadro de los dominios interrelacionados de COBIT[9]



- Planear y Organizar (PO): Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- Adquirir e Implementar (AI): Proporciona las soluciones y las pasa para convertirlas en servicios.
- Entregar y Dar Soporte (DS): Recibe las soluciones y las hace utilizables por los usuarios finales.
- Monitorear y Evaluar (ME): Monitorear todos los procesos para asegurar que se sigue la dirección provista.

- **Planificación y organización:**

[9] http://cs.uns.edu.ar/~ece/auditoria/COBIT-CURNE-UASD

PO1 Definir un plan estratégico de TI
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica
PO4 Definir los procesos, organización y relaciones de TI
PO5 Administrar la inversión en TI
PO6 Comunicar las aspiraciones y la dirección de la gerencia
PO7 Administrar recursos humanos de TI
PO8 Administrar la calidad
PO9 Evaluar y administrar los riesgos de TI
PO10 Administrar proyectos

- **Adquisición e implantación**

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

- **Soporte y Servicios**

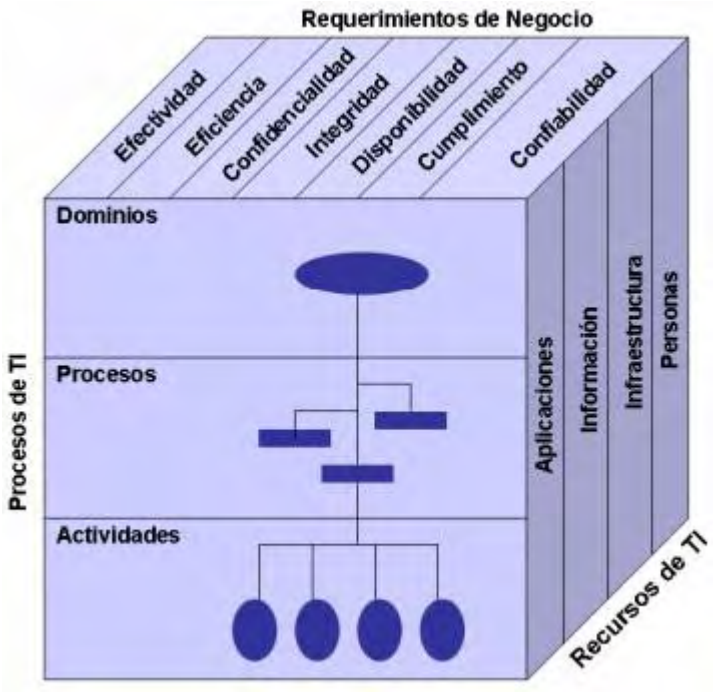
DS1 Definir y administrar los niveles de servicio
DS2 Administrar los servicios de terceros
DS3 Administrar el desempeño y la capacidad
DS4 Garantizar la continuidad del servicio
DS5 Garantizar la seguridad de los sistemas
DS6 Identificar y asignar costos
DS7 Educar y entrenar a los usuarios
DS8 Administrar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

- **Monitoreo y evaluación**

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

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

Figura 3. El cubo de COBIT[10]



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

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

COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es

[10] http://cs.uns.edu.ar/~ece/auditoria/COBIT-CURNE-UASD

necesario que apliquen todas, y, aún más, se pueden combinar como se necesite por cada empresa.

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

Procesos:

PO1 Definición de un plan estratégico:

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros. Su realización se concreta a través de un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

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

PO2 Definición de la arquitectura de información:

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

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

PO3 Determinación de la dirección tecnológica:

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

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI:

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

- El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- Propiedad, custodia, la gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.
- Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

- Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.
- La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.
- El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5 Manejo de la inversión:

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

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

PO6 Comunicación de la dirección y aspiraciones de la gerencia:

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

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido y promovido por la Alta Gerencia.
- Las directrices tecnológicas.

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

PO7 Administración de recursos humanos:

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

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

PO8 Asegurar el cumplimiento con los requerimientos externos:

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

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
- Leyes, regulaciones y contratos.
- Revisiones regulares en cuanto a cambios.

- Búsqueda de asistencia legal y modificaciones.
- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- Privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

PO9 Evaluación de riesgos:

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI. Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

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

PO10 Administración de proyectos:

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión. Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto

emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- Presupuestos de costos y horas hombre.
- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- Plan de administración de riesgos para eliminar o minimizar los riesgos.
- Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad:

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

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

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

Procesos:

AI1 Identificación de soluciones automatizadas:

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

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

AI2 Adquisición y mantenimiento del software aplicativo:

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio. Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

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

AI3 Adquisición y mantenimiento de la infraestructura tecnológica:

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

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

AI4 Desarrollo y mantenimiento de procedimientos:

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

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

AI5 Instalación y aceptación de los sistemas:

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

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

AI6 Administración de los cambios:

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

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

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

Procesos:

Ds1 Definición de niveles de servicio:

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

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

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

Ds2 Administración de servicios prestados por terceros:

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

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

Ds3 Administración de desempeño y capacidad:

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

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- Monitoreo y reporte de los recursos de tecnología de información.
- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.
- Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

Ds4 Asegurar el servicio continuo:

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de Severidad
- Plan Documentado
- Procedimientos Alternativos
- Respaldo y Recuperación
- Pruebas y entrenamiento sistemático y singulares

Ds5 Garantizar la seguridad de sistemas:

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.
- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.

- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización.

Ds6 Educación y entrenamiento de usuarios:

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

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

Ds7 Identificación y asignación de costos:

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI. Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

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

Ds8 Apoyo y asistencia a los clientes de TI:

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente. Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

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

Ds9 Administración de la configuración:

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios. Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

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

Ds10 Administración de problemas:

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder. Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

Ds11 Administración de datos:

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CD y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa. La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

Ds12 Administración de las instalaciones:

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física. Ds13 Administración de la operación Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

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

Procesos:

M1 Monitoreo del proceso:

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos. Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2 monitorear y evaluar el control interno:

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3 garantizar el cumplimiento con requerimientos:

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo. Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4 proporcionar gobierno de TI:

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello

la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría. La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoría, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo. Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente. Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán". Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI". En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista: -Los recursos de las TI. -Los criterios empresariales que deben satisfacer la información. -Los procesos de TI.

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

2. DESARROLLO DE LA AUDITORÍA

2.1. METODOLOGÍA

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

Es responsabilidad de la administración el contenido de la información suministrada por la empresa y analizada por Jhoana Lorena Hernández Benavides, estudiante de la Universidad de Nariño.

Para alcanzar los objetivos propuestos, se utilizó la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

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

ETAPA 1: FAMILIARIZACION CON EL ENTORNO:

Este primer paso se realizó con el fin de familiarizarse con la infraestructura tecnológica de la empresa DISPROPN S.A.S, se hace un estudio previo de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoría, también en esta etapa se definen que elementos se utilizaron para elaborar la auditoría.

Se realizó un trabajo constante en la sede principal DISPROPN S.A.S con el fin de conocer y observar los diferentes procesos, para identificarlos y auditarlos, a través de entrevistas abiertas se dio inicio a la recolección de información, dando el siguiente paso que fueron la aplicación de cuestionarios cuantificables con los funcionarios de los diferentes departamentos, como también la visita a las diferentes sedes que tiene DISPROPAN S.A.S, así:

- Central Pasto
- Ipiales
- Tumaco
- Mocoa
- Puerto Asís

ETAPA 2: PLANEACIÓN DE LAS ACTIVIDADES DE AUDITORÍA

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

- Se realizó un estudio previo de la infraestructura tecnológica de DISPROPAN S.A.S, obteniendo información necesaria respecto al tema.
- Se identifica el alcance y los objetivos de la auditoría a realizar.
- La determinación de los recursos necesarios con los que se realiza la auditoría.
- Se elabora el plan de trabajo.

ETAPA 3: REALIZACIÓN DE LAS ACTIVIDADES DE LA AUDITORÍA

En esta etapa se hicieron efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas seleccionadas que garantizaron el cumplimiento de los objetivos planeados.

Las actividades que se realizaron dentro de esta etapa fueron:

- Elaboración del plan de auditoría, para identificar dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.
- Elaboración de cuadros de definición de fuentes de conocimiento, análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.
- Realización de pruebas sobre los procesos seleccionados.
- Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.
- Identificación de hallazgos dentro del proceso evaluado.
- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.

ETAPA 4: PRESENTACIÓN DEL INFORME FINAL

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

Este informe se presenta y se entrega al gerente de la empresa DISPROPAN S.A.S, para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

3. DESARROLLO DEL TRABAJO

3.1 ARCHIVO PERMANENTE

El archivo permanente contiene información tanto constante como variable en el tiempo. Esta información es de vital importancia y se considera necesaria para comprender en forma exacta, rápida y sencilla las características de las áreas objeto de auditoría.

3.1.1 Dispropan S.A.S.:

Misión:[11] Somos una empresa dedicada a la distribución y comercialización de productos e insumos para el sector Panadero, Pastelero y de Alimentos en los departamentos de Nariño y Putumayo. Ofrecemos un amplio portafolio de productos garantizando calidad, servicio y confiabilidad a nuestros clientes, contribuyendo con el desarrollo de la región y compromiso con el medio ambiente.

Visión: Ser reconocida como una de las empresas líderes en el mercado regional Nariño y Putumayo, enfocado en la consolidación de productos de calidad y la formación de un equipo de trabajo eficiente, innovador y altamente capacitado para responder a las necesidades de nuestros clientes y del mercado en general.

Objeto Social: La sociedad tendrá como objeto principal[12]:

a) Compra y venta de productos e insumos de panadería.
b) El comercio en general al por Mayor y Detal.
c) Compra y venta de mercancías sean nacionales o extranjeras, importación y exportación de materias primas y equipos, en especial productos e insumos para panadería.
d) Transformación de productos de panadería.
e) Elaboración de materias primas e insumos para panadería.
f) Todas las actividades mercantiles, civiles, financieras y accesorias o complementarias que se relacionen directamente con el objeto social; así mismo. Podrá realizar cualquier otra actividad económica lícita tanto en Colombia como en el extranjero. La sociedad podrá llevar a cabo, en general todas las operaciones de cualquier naturaleza que ellas fueren relacionadas con el objeto mencionado, así como cualquier actividad similar, conexa o

[11] http://www.dispropan.com.co/index.php/2012-05-23-21-32-40
[12] Certificación de la Cámara de Comercio CCP-0313787

complementaria o que permitan facilitar o desarrollar el comercio o la industria de la sociedad.

3.2 ARCHIVO CORRIENTE

Para llevar a cabo el proceso de auditoría se hará una recopilación de documentos que tendrán que ver directamente con este desarrollo.

3.2.1 Programa de auditoría. Es importante señalar y detallar el trabajo a realizado, los procedimientos a empleados en la AUDITORÍA INFORMÁTICA A NIVEL DE LOS SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO así, esta auditoría se ejecutó mediante la aplicación de la metodología COBIT (Objetivos de Control para la Información y Tecnologías afines), dentro del cual existen 4 dominios, de los cuales se aplicaran los siguientes:

Objetivos de control para la empresa DISPROPAN S.A.S:

- **Planeación y organización:**

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

Determinación de dirección tecnológica (PO3): se evalúa la determinación de la dirección tecnológica para los planes de adquisición del hardware, donde se evaluara las dependencias de valorización y planeación para que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

- PO3.1 Planeación de la dirección tecnológica: analizar la tecnología existente en cuanto a la infraestructura de las comunicaciones y los servidores.
- PO3.2 Plan de infraestructura tecnológica: verificar que haya un plan de infraestructura tecnológica, evaluar planes de contingencia, evaluar procesos para la adquisición y la evolución de recursos tecnológicos.
- PO3.3 Monitoreo de tendencias y regulaciones futuras: debe existir un proceso para monitorear las directrices del funcionamiento de la infraestructura tecnológica.

- PO3.4 Estándares tecnológicos: evaluar si existen asesorías sobre el funcionamiento de la infraestructura, verificar si existen guías para la selección de la tecnología, medir el cumplimiento de estándares y directrices.

✓ **Evaluación de riesgos (PO9):** el objetivo es asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, mediante la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

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

❖ **Adquisición e implementación:**

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

✓ **Adquisición y mantenimiento de la infraestructura tecnológica (AI3**): el objetivo es proporcionar las plataformas apropiadas para soportar aplicaciones

mediante la realización de una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema.

- AI3.1 Plan de adquisición de infraestructura tecnológica: debe haber un plan que defina la adquisición, el mantenimiento de la infraestructura tecnológica, en este caso, en la parte física de las comunicaciones y de los servidores, un plan que satisfaga los requerimientos funcionales y técnicos de la empresa, se evaluara: En cuanto a comunicaciones y a servidores, la capacidad, vida útil de los equipos tecnológicos, riesgos tecnológicos para la actualización de la tecnología al añadir capacidad técnica, proveedores de Red (Aprobados).
- AI3.2 Protección y disponibilidad del recurso de infraestructura: para proteger los recursos tecnológicos, la empresa debe implementar medidas de control interno, seguridad y adaptabilidad durante la configuración, integración y mantenimiento de la infraestructura como es en este caso el hardware de los equipos de comunicación y de los servidores, que garanticen la disponibilidad e integridad de los recursos tecnológicos. Se debe monitorear y evaluar el uso y las responsabilidades de la utilización que se dé a estos componentes de infraestructura.
- AI3.3 Mantenimiento de la infraestructura: la empresa debe desarrollar una estrategia de actualización y un plan de mantenimiento de la infraestructura, garantizar el control de los cambios de infraestructura tecnológica, incluir una revisión periódica contra las necesidades de la empresa, riesgos, identificar vulnerabilidades.
- AI3.4 Ambiente de prueba de factibilidad: evaluar la efectividad y eficacia de la infraestructura, sobre todo en los procesos de adquisición, funcionalidad, configuración de hardware, pruebas de desempeño, estructura de Red.

✓ **Instalación y aceptación de los sistemas (AI5)** el objetivo es verificar y confirmar que la solución sea adecuada para una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas. Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.

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

- AI5.4 Adquisición de recursos de TI: se debe proteger y cumplir los intereses de la empresa en todos los contratos de adquisición de infraestructura tecnológica, incluyendo los derechos y obligaciones de las partes en los términos contractuales.

❖ **Entrega de servicios y soporte**

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

Garantizar la seguridad de sistemas (Ds5) salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- DS5.1 Administración de la seguridad de TI: administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
- DS5.2 Plan de seguridad de TI: trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.
- DS5.3 Administración de identidad: todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.
- DS5.4 Administración de cuentas del usuario: garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios,

incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad: garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser re acreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.
- DS5.6 Definición de incidente de seguridad: garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.
- DS5.7 Protección de la tecnología de seguridad: garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.
- DS5.8 Administración de llaves criptográficas: determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.
- DS5.9 Prevención, detección y corrección de software malicioso: garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).
- DS5.10 Seguridad de la red: garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

- DS5.11 Intercambio de datos sensitivos: garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

✓ **Administración de la configuración (DS9):** el objetivo es dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios realizando controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

- DS9.1 Repositorio de configuración y línea base: establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.
- DS9.2 Identificación y mantenimiento de elementos de configuración: contar con procedimientos en orden para:
  - Identificar elementos de configuración y sus atributos
  - Registrar elementos de configuración nuevos, modificados y eliminados
  - Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones
  - Actualizar los elementos de configuración existentes en el repositorio de configuraciones
- Prevenir la inclusión de software no-autorizado
- Estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones sobre el repositorio de configuración y estar integrados de forma apropiada con los procedimientos de administración de cambios y administración de problemas.
- DS9.3 Revisión de integridad de la configuración: revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse. Entregar y dar soporte.

- ✓ **Administración de datos (Ds11):** asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

- DS11.2 Acuerdos de almacenamiento y conservación: definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encripción y autenticación.
- DS11.3 Sistema de administración de librerías de medios: definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.
- DS11.4 Eliminación: definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse.
- DS11.5 Respaldo y restauración: 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.
- DS11.6 Requerimientos de seguridad para la administración de datos: establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

- ✓ **Administración de las instalaciones (Ds12**): proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que

provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- DS12.1 Selección y Diseño del Centro de Datos: el área de sistemas debe definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia empresarial. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
- DS12.3 Acceso Físico: la empresa debe definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.
- DS12.5 Administración de instalaciones físicas: se debe administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y de la empresa, las especificaciones del proveedor y los lineamientos de seguridad y salud.

✓ **Administración de la operación (Ds13):** asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- DS13.3 Monitoreo de la infraestructura de TI: definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.
- DS13.5 Mantenimiento preventivo del hardware: definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

❖ **Monitoreo y evaluación (ME)**

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

✓ **Monitorear y evaluar el control interno (M2):** asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

- ME2.1 Monitoreo del marco de trabajo de control interno: deberá monitorear de forma continua, comparar y mejorar el ambiente de control de TI (infraestructura de la Red y de los equipos utilizados como servidores) y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.
- ME2.6 Control interno para terceros: evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicios externos cumplen con los requerimientos legales y regulatorios y obligaciones contractuales.
- ME2.7 Acciones correctivas: identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

3.2.2 Diseño de los elementos de auditoría: para el desarrollo de la auditoría que permita evaluar la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, servidores y el funcionamiento del sistema SYSCAFE para la empresa DISPROPAN S.A.S. se utilizan los siguientes formatos de recolección de información.

Para dar comienzo a la auditoría, se realizaron diferentes entrevistas con el personal de la empresa, gerente y administrativos, información que sirve para el reconocimiento de los diferentes procesos, por tanto información clave para el desarrollo de este trabajo.

❖ **Cuadro de definición de fuentes de conocimiento**, pruebas de análisis, y pruebas de auditoría: Este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso

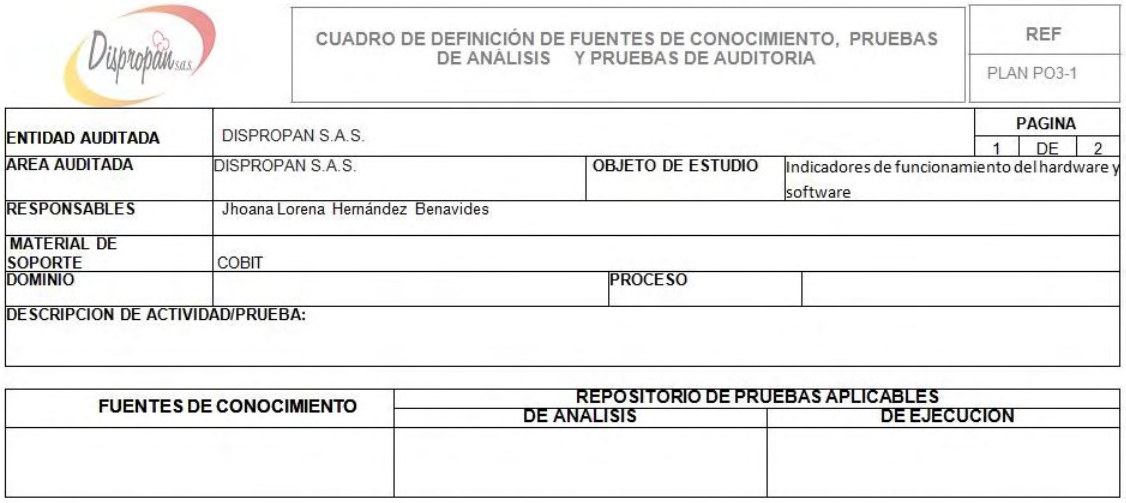
dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

- ✓ **REF**: identificación del cuadro de definición.
- ✓ **ENTIDAD AUDITADA**: en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ✓ **PROCESO AUDITADO:** en este espacio se indicara el nombre del proceso objeto de la auditoría.
- ✓ **RESPONSABLES:** nombre del auditor o auditores.
- ✓ **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** en este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ✓ **MATERIAL DE SOPORTE:** en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **DOMINIO**: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- ✓ **PROCESO:** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- ✓ **FUENTES DE CONOCIMIENTO**: espacio que permite identificar las herramientas necesarias para obtener la información, puede ser a través de entrevistas, manuales, política, archivos físicos o magnéticos, reportes, contratos, etc.
- ✓ **REPOSITORIO DE PRUEBAS**: se divide en dos tipos de pruebas:

- Repositorio de pruebas de análisis: espacio en el que describe el análisis de cada proceso y de la información obtenida.
- Repositorio de pruebas de ejecución: se describe las acciones a realizar para la ejecución de la auditoría, como las revisiones, verificaciones, pruebas y obtención de inconsistencias, etc

Figura 4. Cuadro de definición de fuentes de conocimiento



	CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA	REF
		PLAN PO3-1

				PAGINA
ENTIDAD AUDITADA	DISPROPAN S.A.S.			1 DE 2
AREA AUDITADA	DISPROPAN S.A.S.	OBJETO DE ESTUDIO	Indicadores de funcionamiento del hardware y software	
RESPONSABLES	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		PROCESO		
DESCRIPCION DE ACTIVIDAD/PRUEBA:				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	DE EJECUCION

Pruebas de análisis de auditoría: el desarrollo de los cuadros de definición de fuentes de conocimiento, pruebas de análisis de auditoría se encuentran en la carpeta de anexos/cuadros de definición.

- **Cuestionario cuantitativo:** el cuestionario cuantitativo permite dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su vulnerabilidad.

Este cuestionario cuantitativo está conformado por los siguientes ítems:

- ✓ **REF**: identificación del cuadro de definición.
- ✓ **ENTIDAD AUDITADA**: en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ✓ **PROCESO AUDITADO:** en este espacio se indicara el nombre del proceso objeto de la auditoría.
- ✓ **RESPONSABLES:** nombre del auditor o auditores.
- ✓ **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** en este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ✓ **MATERIAL DE SOPORTE:** en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **DOMINIO**: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- ✓ **PROCESO:** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- ✓ **PREGUNTA:** planteamiento de la descripción de la información requerida a evaluar.

- ✓ **SI – NO: SI-NO-NA:** de acuerdo a un puntaje de 1 a 5 (donde 1 es el puntaje mínimo que se le puede asignar con significado irrelevante y 5 es el puntaje máximo con significado de alta importancia) se evalúa si cumple o no con la información requerida.
- ✓ **FUENTE:** fuente de donde se obtiene la información requerida
- ✓ **TOTAL:** se asigna los valores correspondientes a cada columna la sumatoria de los SI, la sumatoria de los NO y la sumatoria de los NA.
- ✓ **TOTAL CUESTIONARIO:** la sumatoria de los SI + NO + NA.
- ✓ **PORCENTAJE DE RIESGO:** hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

Figura 5. Cuestionario cuantitativo.

	CUESTIONARIO CUANTITATIVO	REF

ENTIDAD AUDITADA	DISPROPAN S.A.S.			**PAGINA**	
				1	DE 1
PROCESO AUDITADO	Eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, servidores y el funcionamiento del sistema SYSCAFE				
RESPONSABLE	Jhoana Lorena Hernández Benavides				
MATERIAL DE SOPORTE		COBIT			
DOMINIO		**PROCESO**			

PREGUNTA	SI	NO	NA	FUENTE
1. ¿?				
2. ¿?				
TOTALES				
TOTAL CUESTIONARIO				

PORCENTAJE DE RIESGO

AUDITOR RESPONSABLE
Jhoana Lorena Hernández Benavides

El Desarrollo de los cuestionarios cuantitativos se encuentra en la carpeta de anexos/cuestionarios.

ENTREVISTAS

❖ **Entrevistas preguntas abiertas y preguntas cerradas:**

Técnica utilizada para la recolección de información amplia que permita aclarar dudas que dejan los cuestionarios. Los formatos utilizados para hacer las entrevistas están ajustados al personal del área de Sistemas, al personal técnico y en general a todo el personal involucrado en el personal del área de tecnologías de la Información y Comunicación. Se realizaron dos tipos de entrevistas: Entrevistas con preguntas Abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una. Entrevistas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

Formatos presentados en la siguiente página así:

PLAN	REF

ENTIDAD AUDITADA	DISPROPAN S.A.S.	**PAGINA**		
		1	DE	1
PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software			
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE		COBIT		
DOMINIO		**PROCESO**		

ENTREVISTADO	
CARGO	

1. ¿Las características del equipo son suficientes para el desempeño de su trabajo?

   _____

2. ¿Qué hace en caso de que el equipo falle? ¿a quién acude? _____

_____

3. ¿Cuántos Mantenimiento se le han realizado al equipo?_____
4. ¿Qué nivel de conocimientos tiene en el manejo de un Computador y/o Móvil?

_____

5. ¿Ud. maneja el software de SYSCAFE?_____
6. ¿Ud. Ha recibido asesoramiento o capacitación sobre el manejo de SYSCAFE?

_____

7. ¿Qué procesos de SYSCAFE utiliza?

_____

8. ¿Conoce y ha hecho uso del manual de SYSCAFE?

_____

9. ¿Ha tenido problemas con el Software SYSCAFE? ¿Cuáles?_____

_____

10. ¿Cómo resuelve los problemas encontrados en el Software SYSCAFE?_____
11. ¿Cuál es el tiempo máximo en solucionar el problema de SYSCAFE?_____

NOMBRE AUDITOR RESPONSABLE FIRMA
Jhoana Hernández B.

- **Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso**

Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

Tabla 1. Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

PROBABILIDAD	ALTO 61-100%	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE	ZONA DE RIESGO INACEPTABLE
	MEDIO 31-60%	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE
	BAJO 0-30%	ZONA DE RIESGO ACEPTABLE	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO
		BAJO (LEVE)	MEDIO (MODERADO)	ALTO (CATASTROFICO)
	IMPACTO			

3.2.3 Análisis y evaluación riesgos preliminares:

Manual de navegación de hallazgos: en este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

REF: se refiere al ID del elemento.

ENTIDAD AUDITADA: en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: en este espacio se indicara el nombre del proceso objeto de la auditoría.

RESPONSABLES: en este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

HALLAZGO: aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

CONSECUENCIAS Y RIESGOS: en este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

EVIDENCIAS: aquí encontramos en nombre de la evidencia y el número del anexo donde ésta se encuentra.

RECOMENDACIONES: en este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

	HALLAZGO DISPROPAN	**REF**

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**		
		1	DE	1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		
HALLAZGO				

IMPACTO

RECOMENDACIÓN:

PROBABILIDAD – IMPACTO			
Probabilidad		**Impacto**	

Dominio en ejecución DS5
Garantizar la seguridad del sistema

	CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA	REF
		PLAN DS5

ENTIDAD AUDITADA	DISPROPAN S.A.S.		**PAGINA** 1 DE 1	
ÁREA AUDITADA	DISPROPAN S.A.S.	**OBJETO DE ESTUDIO**	Indicadores de funcionamiento del hardware y software	
RESPONSABLES	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Dar soporte y servicio (DS)	**PROCESO**	Garantizar la seguridad de sistemas(DS5)	
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: El objetivo es salvaguardar la información contra uso no autorizado, divulgación, modificación, daño o pérdida.				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Administrar la seguridad de TI al nivel más apropiado dentro de la empresa. • Plan de seguridad de TI. • Administrar la identidad de todos los usuarios y su actividad de sistemas. • Administración de cuentas de usuario y la persona encargada de suministrar los privilegios de acceso. • Plan de prevención, detección y corrección de software malicioso.	• Analizar la metodología de seguridad de TI. • Analizar la actualización y el control de los planes seguridad de TI. • Analizar la metodología de identidad de usuarios. • Analizar la metodología del manejo de cuentas de usuarios y privilegios de acceso.	• Revisión de la metodología de seguridad de TI. • Revisión del manejo de identidad de usuarios. • Revisión del acceso y privilegios de usuarios.

AUDITOR RESPONSABLE Jhoana Lorena Hernández Benavides

	CUESTIONARIO CUANTITATIVO	REF
		DS5-1-2

ENTIDAD AUDITADA	DISPROPAN SAS				**PAGINA**	
					1 DE 2	
ÁREA AUDITADA	DISPROPAN SAS	**OBJETO DE ESTUDIO**	Indicadores de funcionamiento del hardware y software			
RESPONSABLES	Jhoana Lorena Hernández Benavides					
MATERIAL DE	COBIT					
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (Ds5)			

PREGUNTA	SI	NO	NA	**FUENTE**
1. ¿En DISPROPAN SAS existen procedimientos o metodologías para mantener la seguridad de la Infraestructura Tecnológica?		5		ENTREVISTA AREA ADMINISTRATIVA
2. ¿El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware?		5		
3. ¿Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios?		4		
4. ¿Existe una administración del acceso del usuario al software SYSCAFE?		5		
5. ¿Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario?		4		
6. ¿Existe un control del manejo de usuarios en el software SYSCAFE?		5		
7. ¿existe una persona encargada de monitorear y evaluar el uso y las responsabilidades de la utilización que se da al manejo del software SYSCAFE?		4		
8. ¿Se evalúa la efectividad y eficacia del software SYSCAFE?		4		

9. Existen documentación de las Garantías, técnicas de seguridad y procedimientos de administración del software SYSCAFE.		3		
TOTAL		39		
TOTAL CUESTIONARIO		39		

PORCENTAJE DE RIESGO: $\frac{0 * 100}{39} = 0$

= 100 - 0

= 100 %

DATOS DEL CUESTIONADO

Nombre	**ANA ROCIO ORTEGA**
Cargo	**ADMINISTRADORA**

AUDITOR RESPONSABLE
JHOANA HERNANDEZ B.

❖ **Entrevista personal de la empresa Dispropan SAS.**

Dispropan

AGENCIA Dispropan
FECHA 17-02-2014
NOMBRE Carolina Hernandez
CARGO Encargada Punto Venta Ipiales

1. ¿En qué consiste su cargo? Ventas, Pedidos, Inventario, Caja, Consignaciones, Compras, Gastos.
2. Describa brevemente el uso que le da al equipo Programa Siscafe. red social, correo electronica
3. Describa brevemente como es el desempeño del equipo que está operando Sin Novedades
4. ¿Considera que las características del hardware del equipo son suficientes para el desempeño de su trabajo? Si
5. ¿Qué hace en caso de que el equipo falle? ¿a quien acude? tecnicos particulares
6. Que nivel de conocimientos tiene en el manejo de un Computador. Alto
7. ¿Ud maneja el software de SYSCAFE? Si
8. Han recibido asesoramiento o capacitación sobre el manejo de SYSCAFE? Si
9. Cual es su nivel de acceso a SYSCAFE registro ventas, Inventarios
10. Conoce y ha hecho uso del manual de SYSCAFE? No
11. Ha tenido problemas con el Software SYSCAFE? Si
12. Como resuelve los problemas encontrados en el Software SYSCAFE. directo/con ellos
13. Ha tenido problemas con la navegación de Internet. No
14. Cuantos Mantenimiento se le han realizado al equipo? 1
15. Se han presentado averías en las instalaciones?. No
16. Se han presentado perdida de información. No
17. Llevan una documentación de planes de contingencia. No
18. Tienen alguna medida de seguridad para la entrada y salida de la agencia. (señales de evacuación, extintor. vigilancia). vigilancia en la noche. extintor si, señales de evacuación No.

	SOFTWARE GESTION SYSCAFE DISPROPAN	**REF**
		SGDD_O6

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**	1 DE 16
RESPONSABLE	Jhoana Lorena Hernández Benavides		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds5)

PERMISOS DEL SOFTWARE GESTION SYSCAFE[13]

Con el fin de tener un acceso controlado al sistema, El software Gestión Comercial Plus SysCafé permite crear usuarios con diferentes niveles de acceso y permisos.

- Código: Número que identificará al usuario en el sistema. Éste aparecerá en los comprobantes que elabore dicho usuario.
- Nombre: identificación del usuario de Gestión Comercial Plus SysCafé. Dicho nombre aparecerá al momento que ingrese al programa.
- Clase: Determina el nivel de acceso que tendrá el usuario:
- Administrador: Tiene acceso a todas las opciones del programa.
- Normal: Puede realizar todos los movimientos, hacer modificaciones a los mismos y generar todos los informes, sin embargo no podrá cambiar los Parámetros de la empresa (Nombre de la empresa, datos de la empresa, etc.) ni podrá crear ni modificar usuarios.
- Auxiliar: Puede realizar movimientos y generar algunos informes, pero no podrá hacer modificaciones a los comprobantes ya elaborados, además de no poder cambiar los Parámetros de la empresa ni crear ni modificar usuarios.
- Invitado: solo tiene acceso a la revisión los movimientos elaborados; no podrá generar comprobantes, hacer modificaciones, cambiar parametrización ni modificar ó crear usuarios.

[13] www.syscafe.com.co/manual

3.3 VISION DE LA INFORMACION DEL SISTEMA Y PERMISOS DEL SOFTWARE

Imagen 1. Información de la empresa

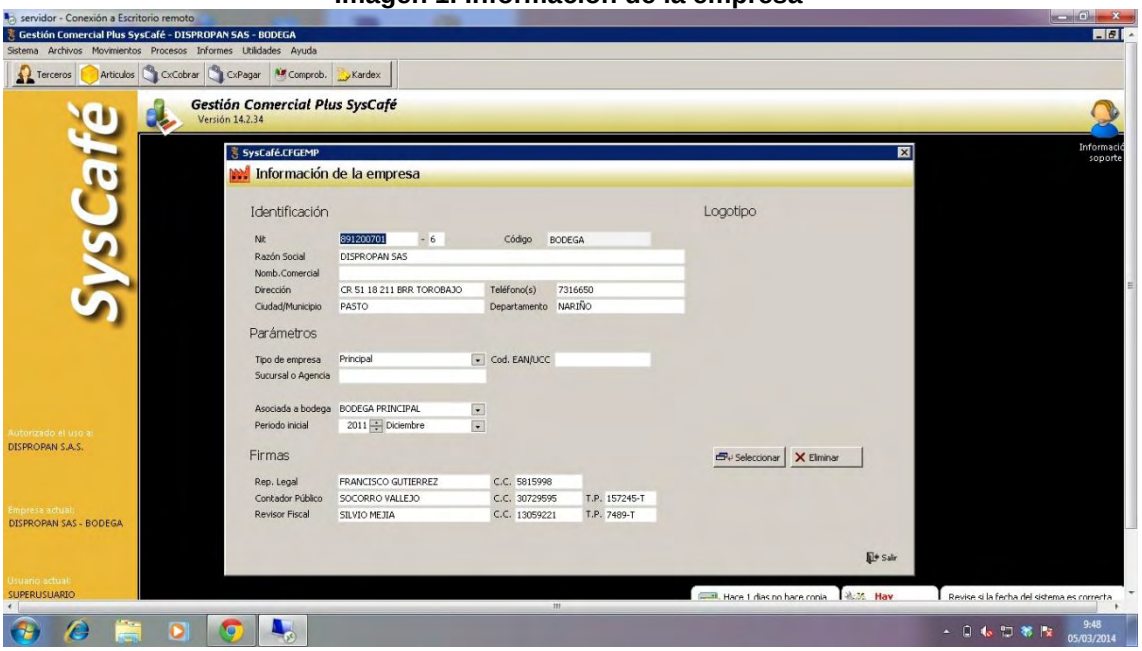


Imagen 2. Información del sistema

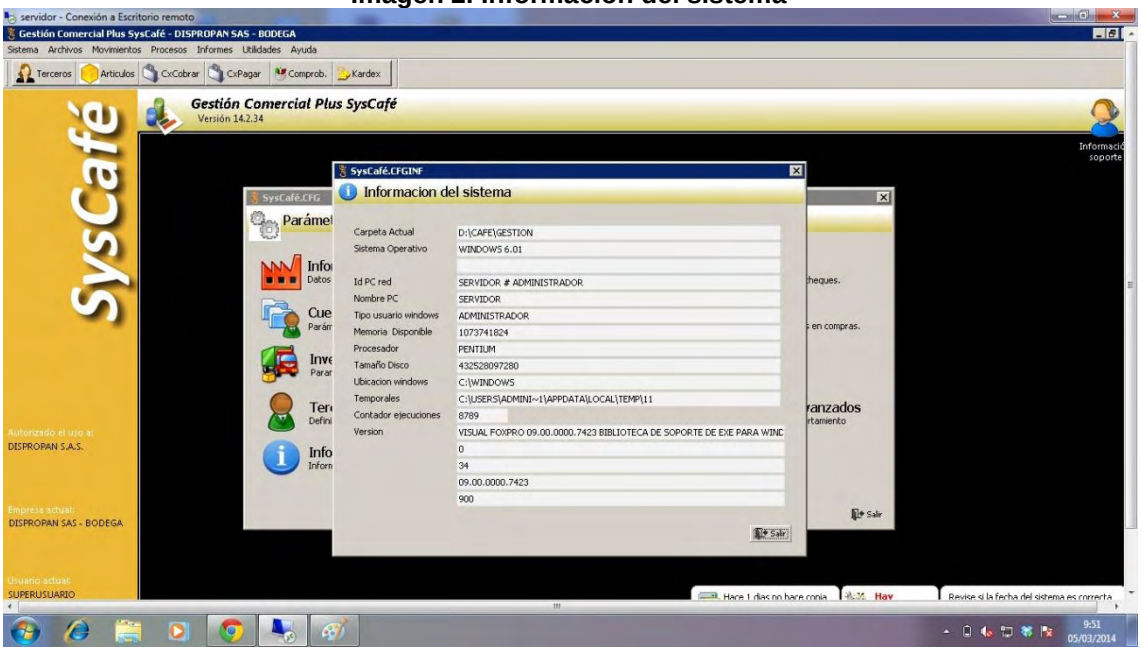


Imagen 3. Permisos y restricciones del usuario superusuario al sistema

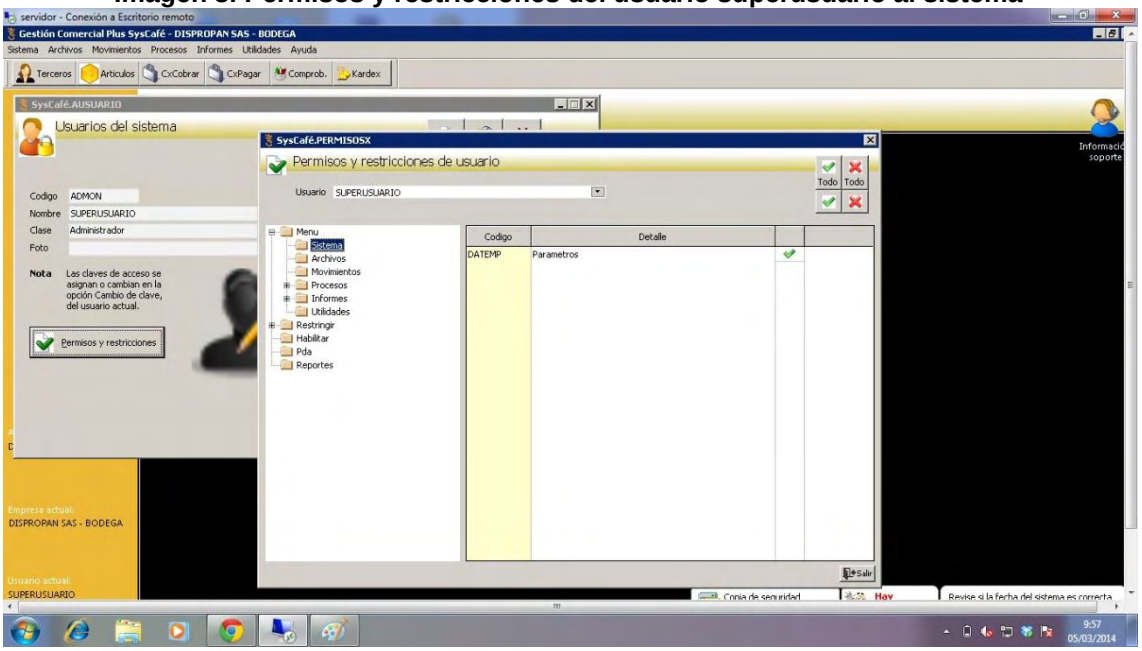


Imagen 4. Permisos y restricciones del usuario superusuario a los archivos

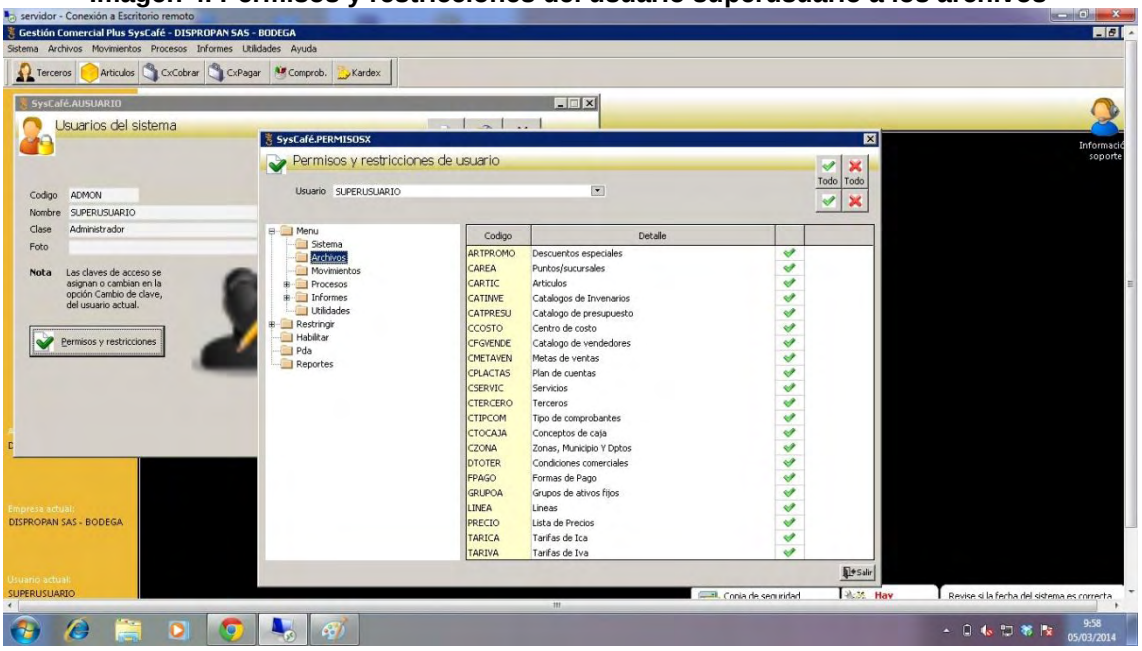


Imagen 5. Permisos y restricciones del usuario superusuario a los movimientos

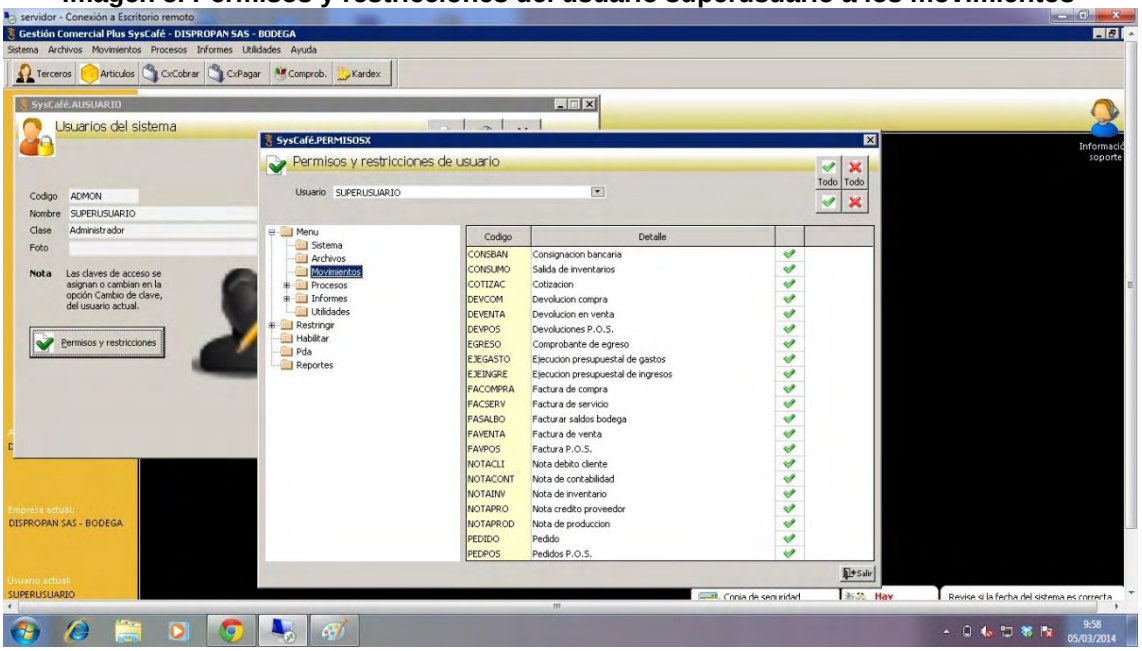


Imagen 6. Permisos y restricciones del usuario superusuario a los procesos

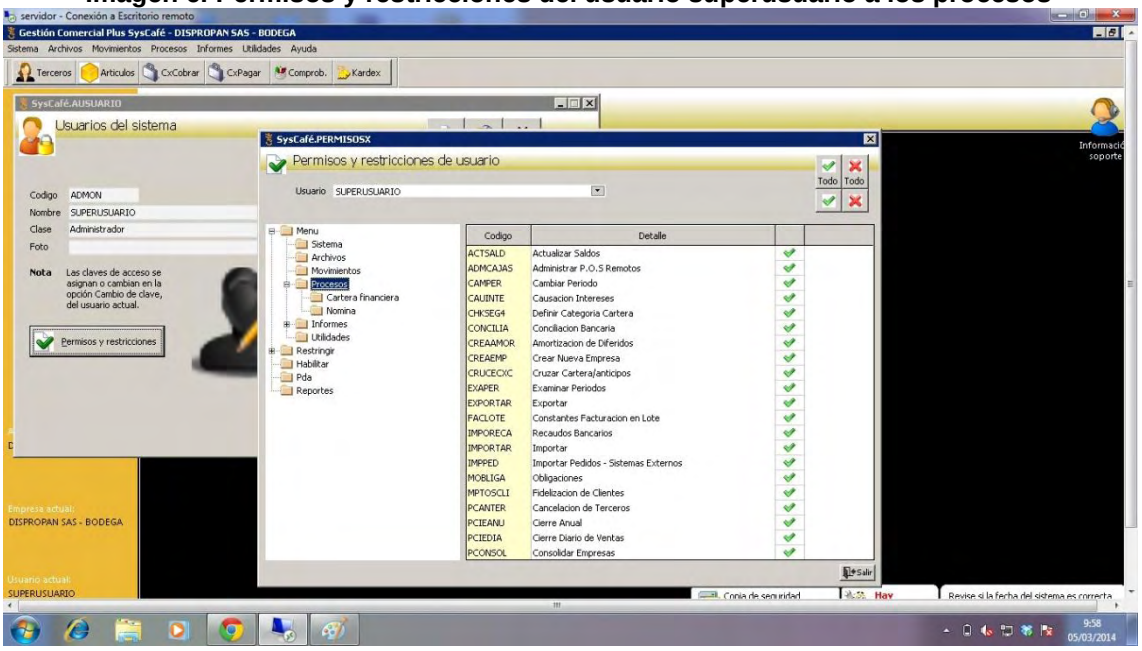


Imagen 7. Permisos y restricciones del usuario superusuario a la cartera financiera

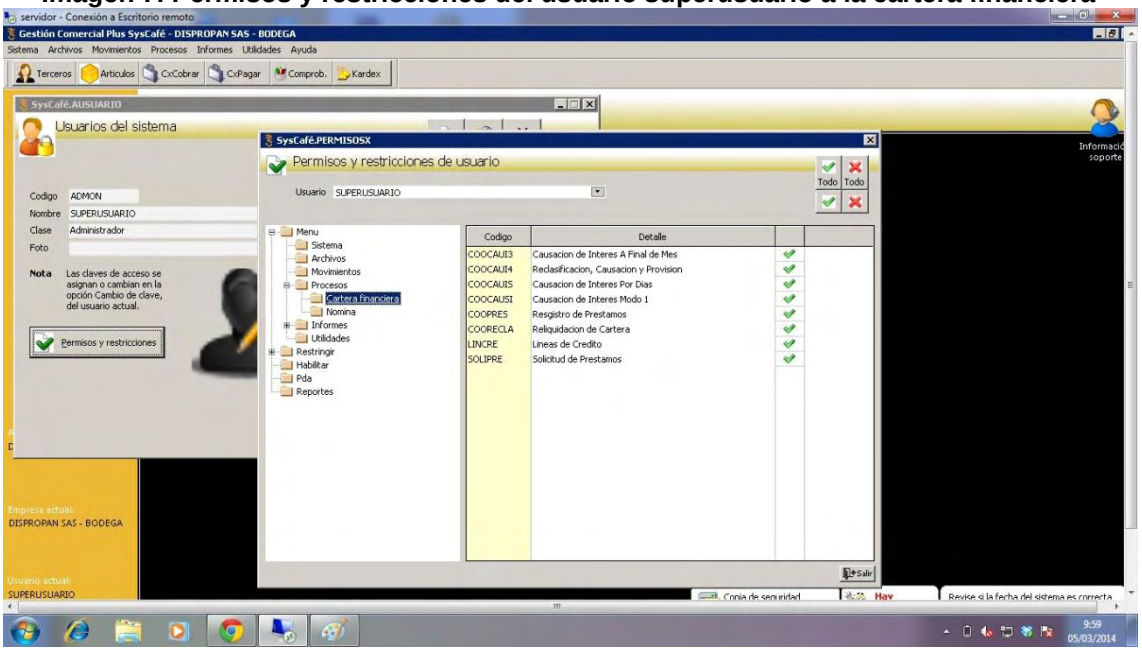


Imagen 8. Permisos y restricciones del usuario superusuario a la nomina

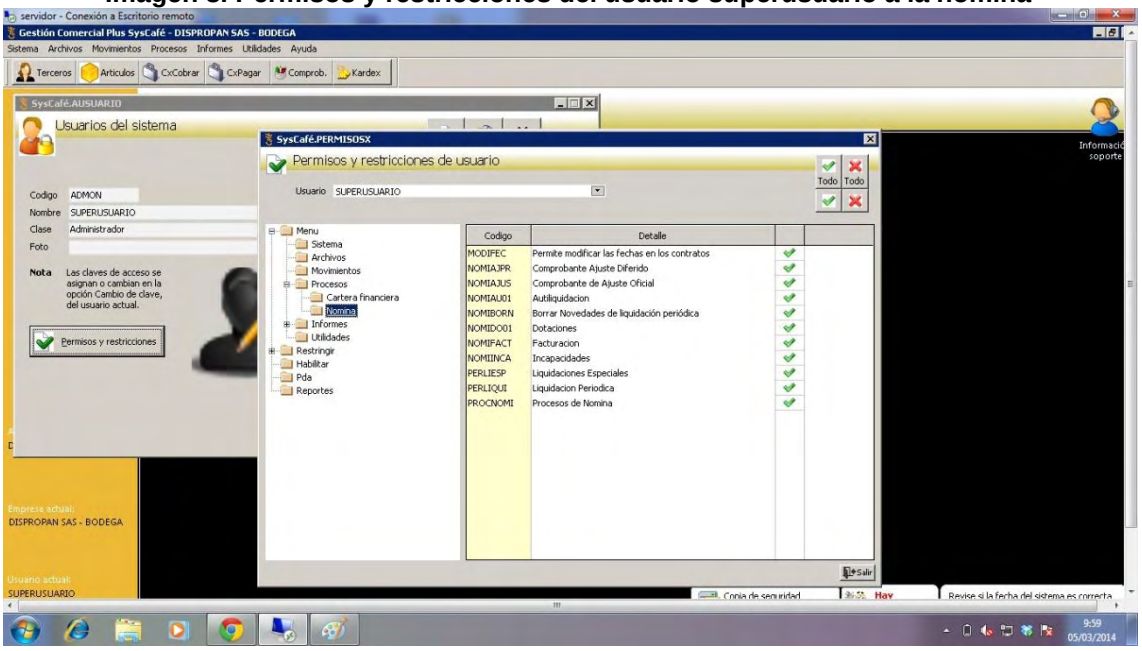


Imagen 9. Permisos y restricciones del usuario superusuario a informes de contabilidad

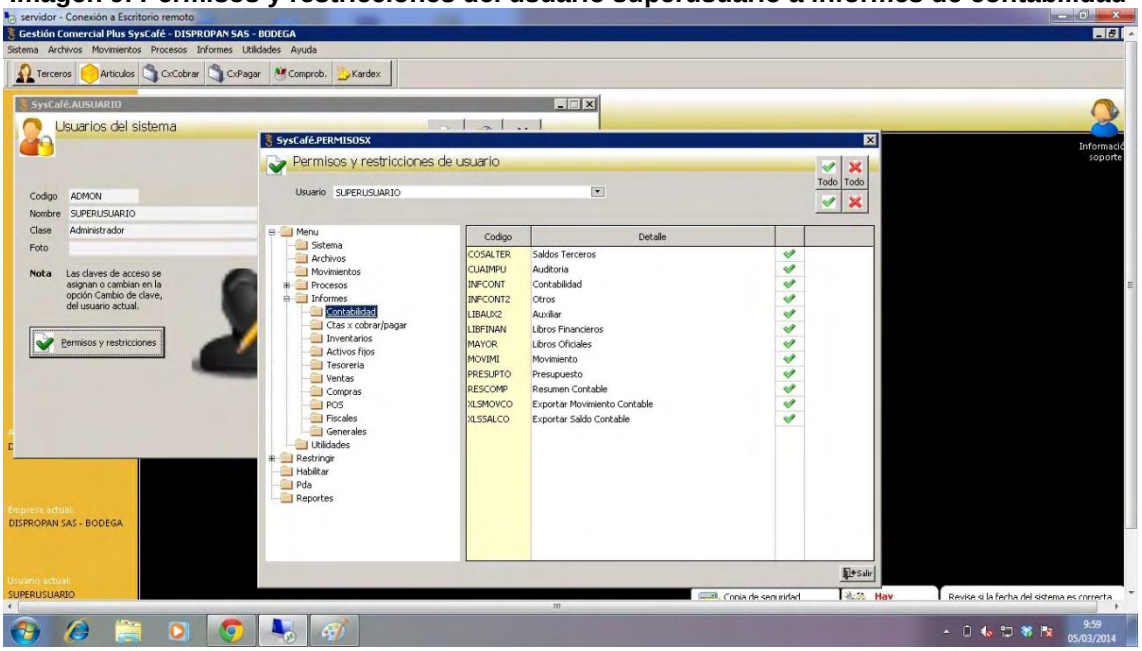


Imagen 10. Permisos y restricciones del usuario superusuario a informes de ctas x cobrar

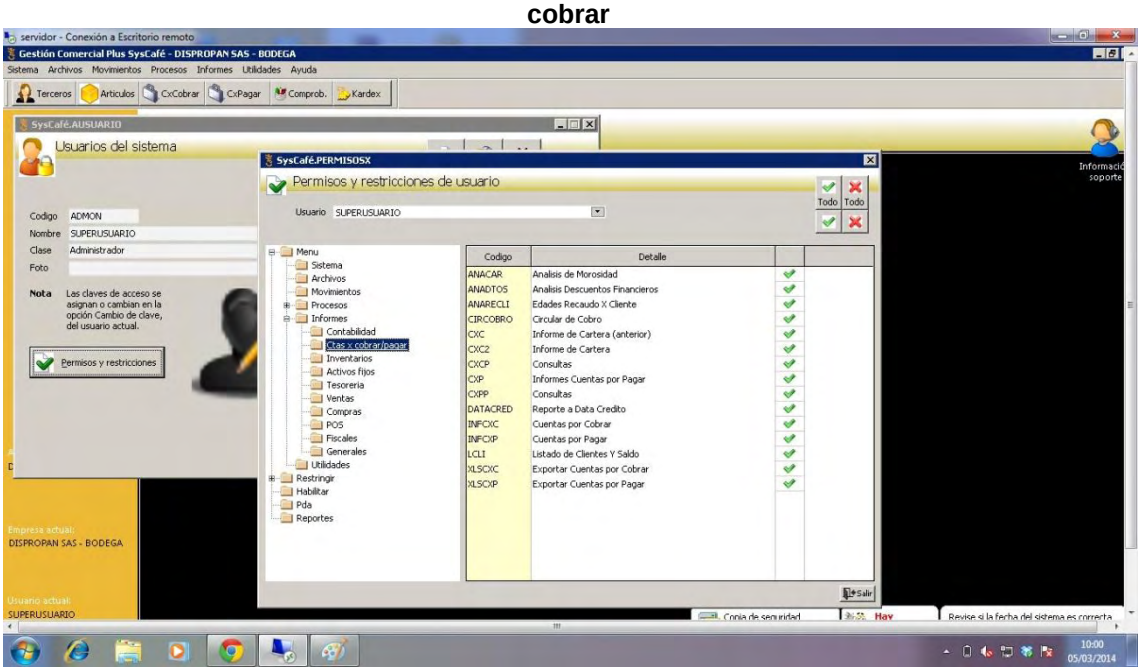


Imagen 11. Permisos y restricciones del usuario superusuario a informes de inventario

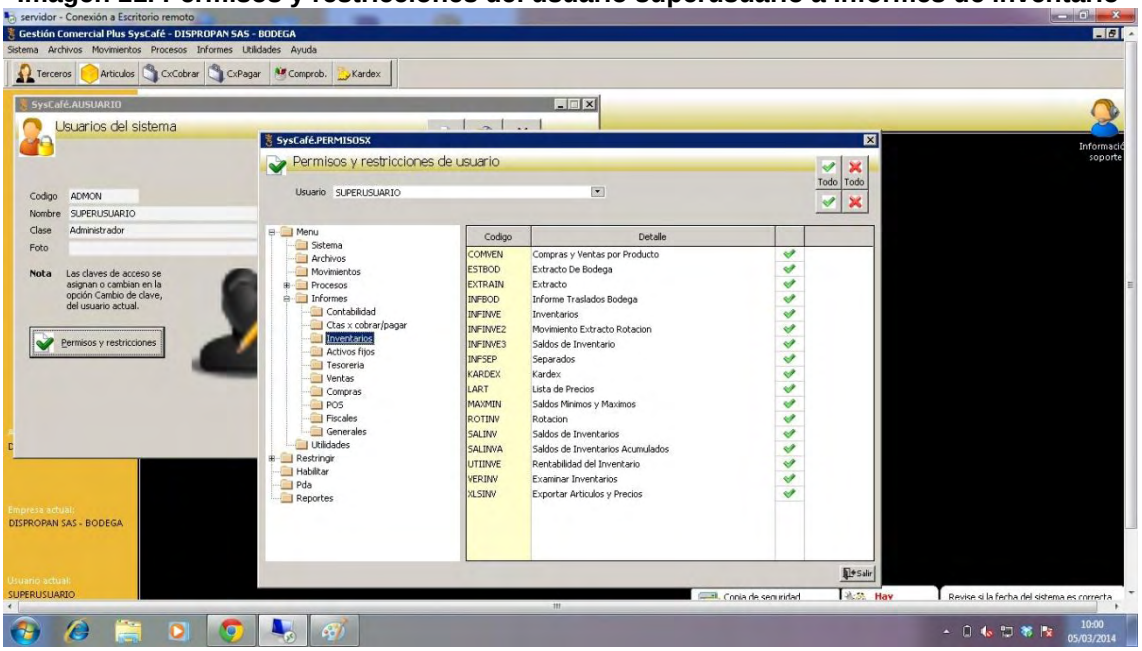


Imagen 12. Permisos y restricciones del usuario superusuario a informes de activos fijos

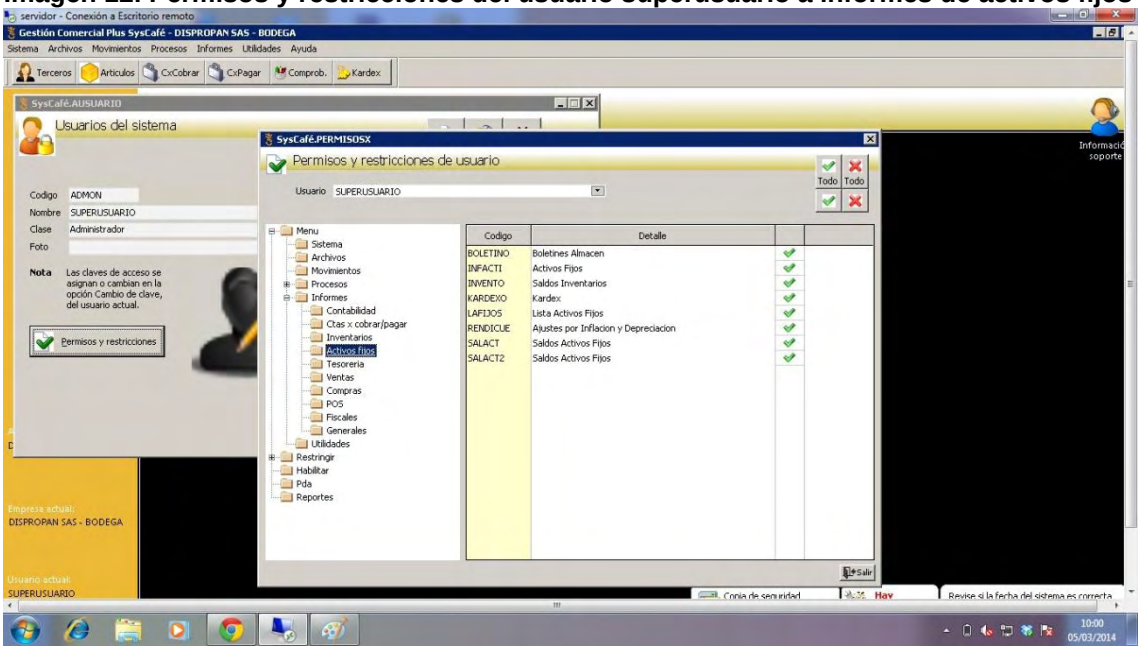


Imagen 13. Permisos y restricciones del usuario superusuario a informes de tesorería

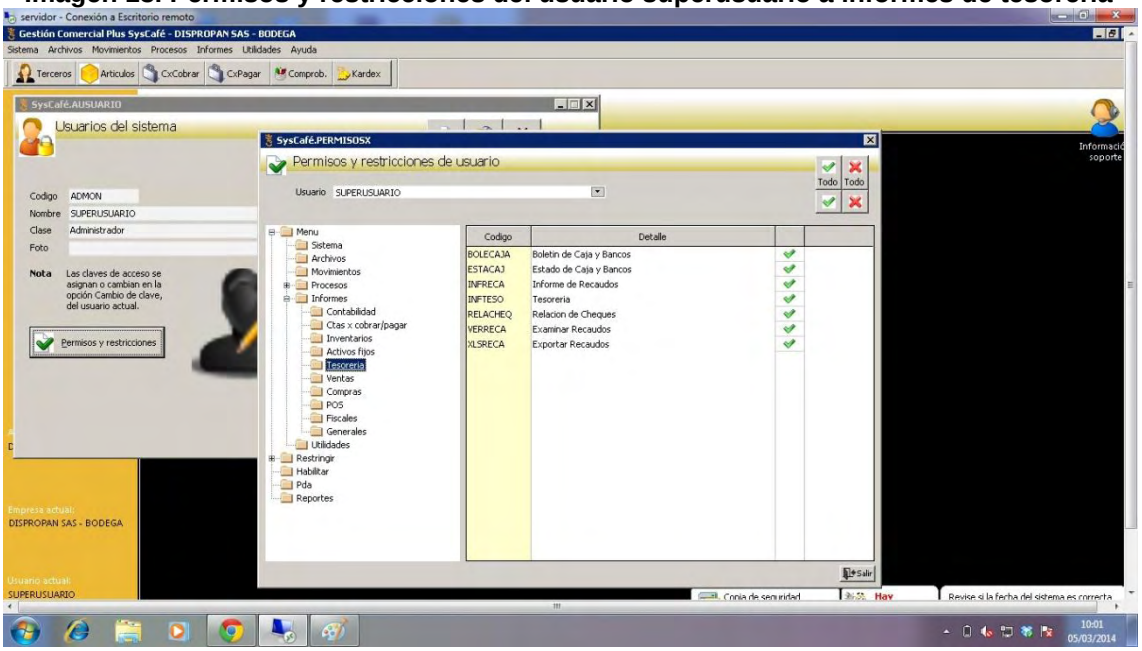


Imagen 14. Permisos y restricciones del usuario superusuario a informes de ventas

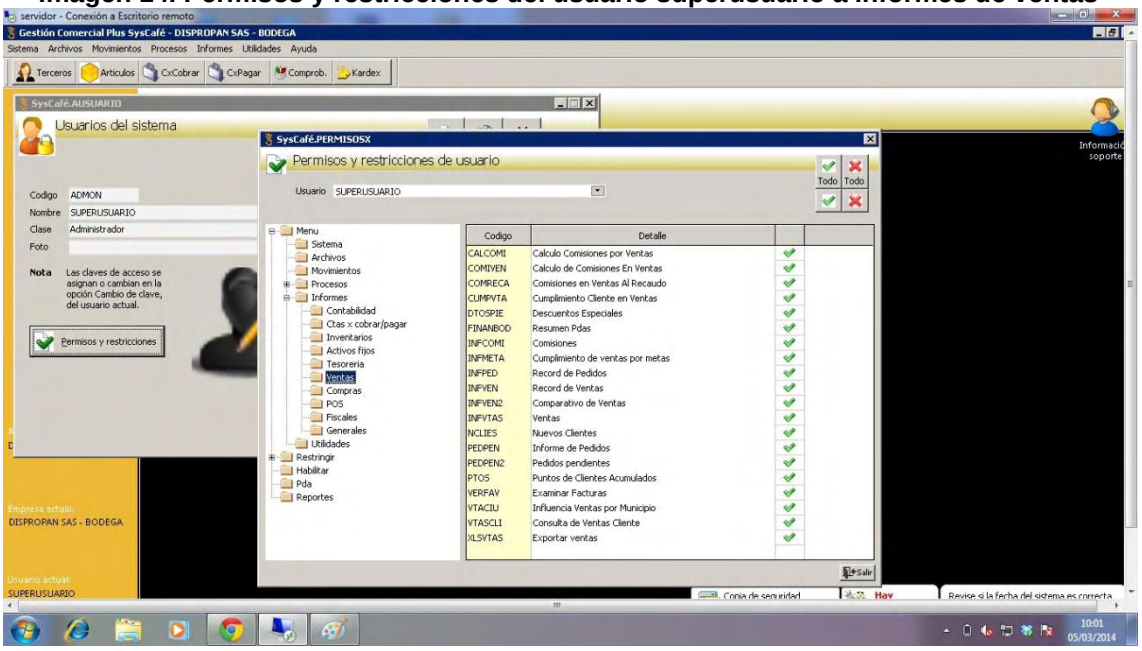


Imagen 15. Permisos y restricciones del usuario superusuario a informes comerciales

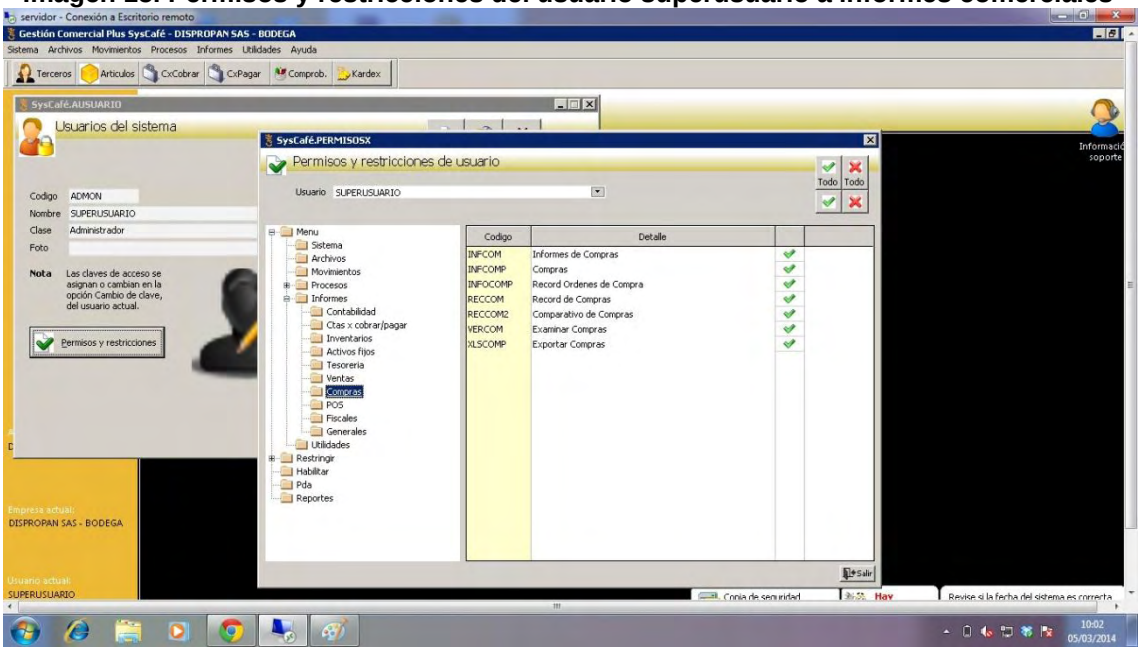


Imagen 16. Permisos y restricciones del usuario superusuario a informes de pos

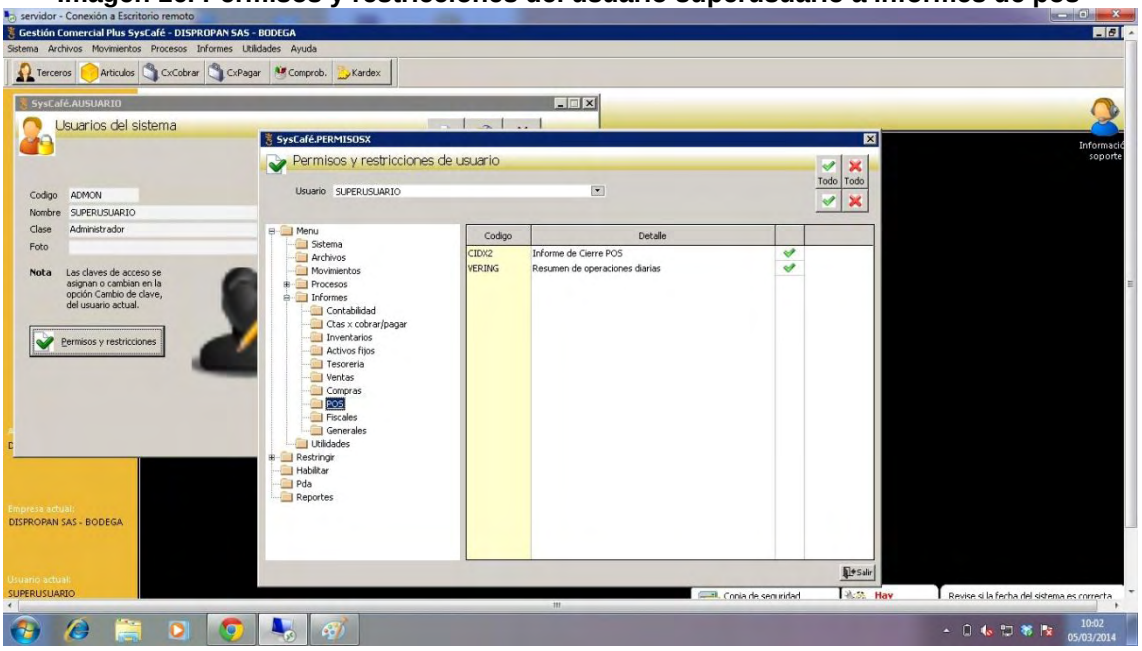


Imagen 17. Permisos y restricciones del usuario superusuario a informes fiscales

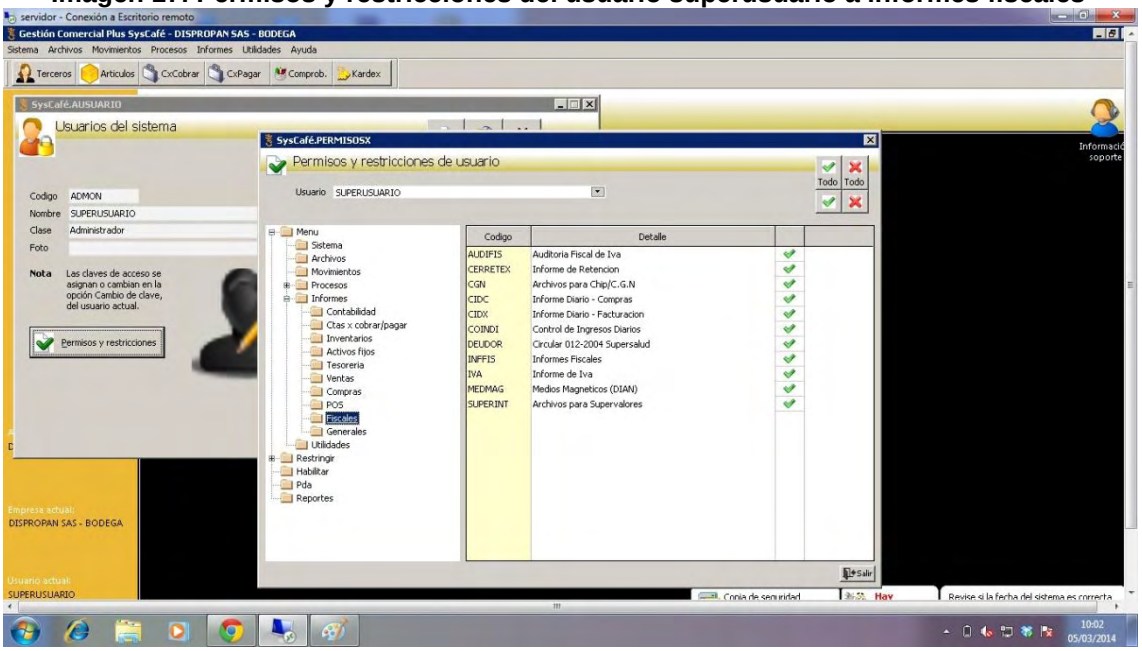


Imagen 18. Permisos y restricciones del usuario superusuario informes generales

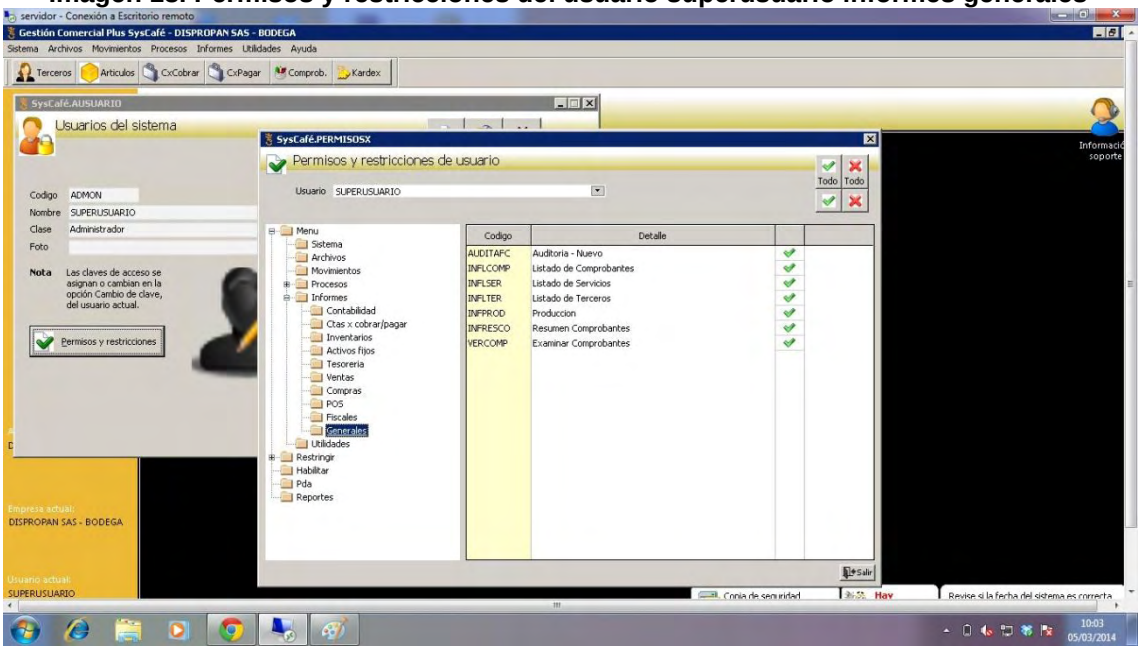


Imagen 19. Permisos y restricciones del usuario superusuario a utilidades del sistema

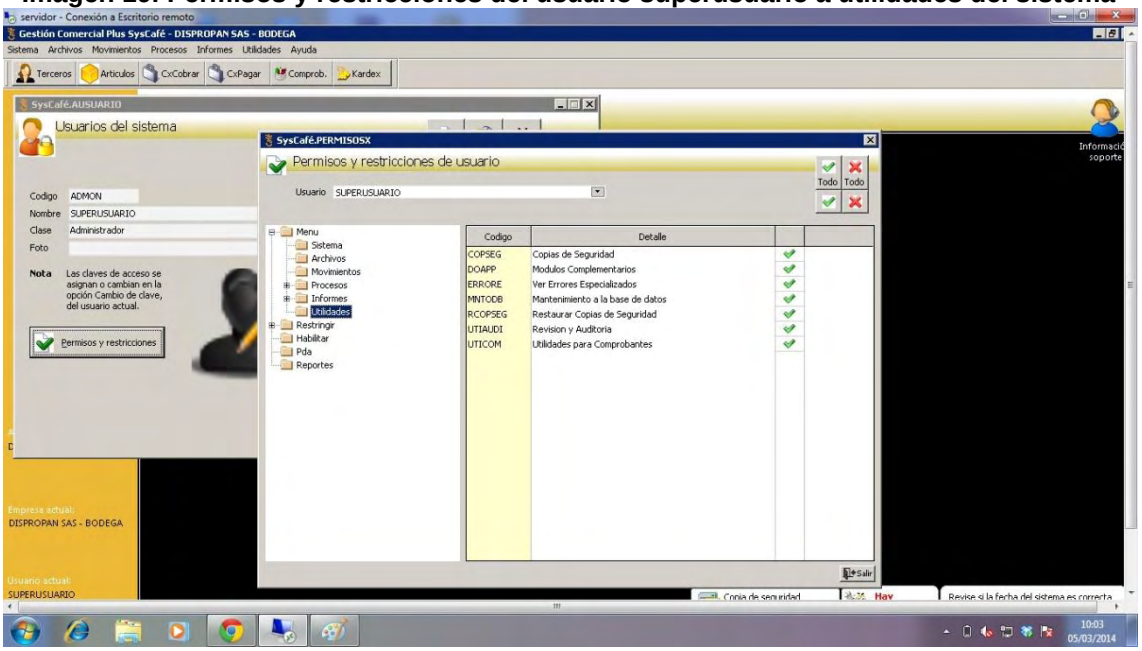


Imagen 20. Permisos y restricciones del usuario superusuario a restringir movimientos

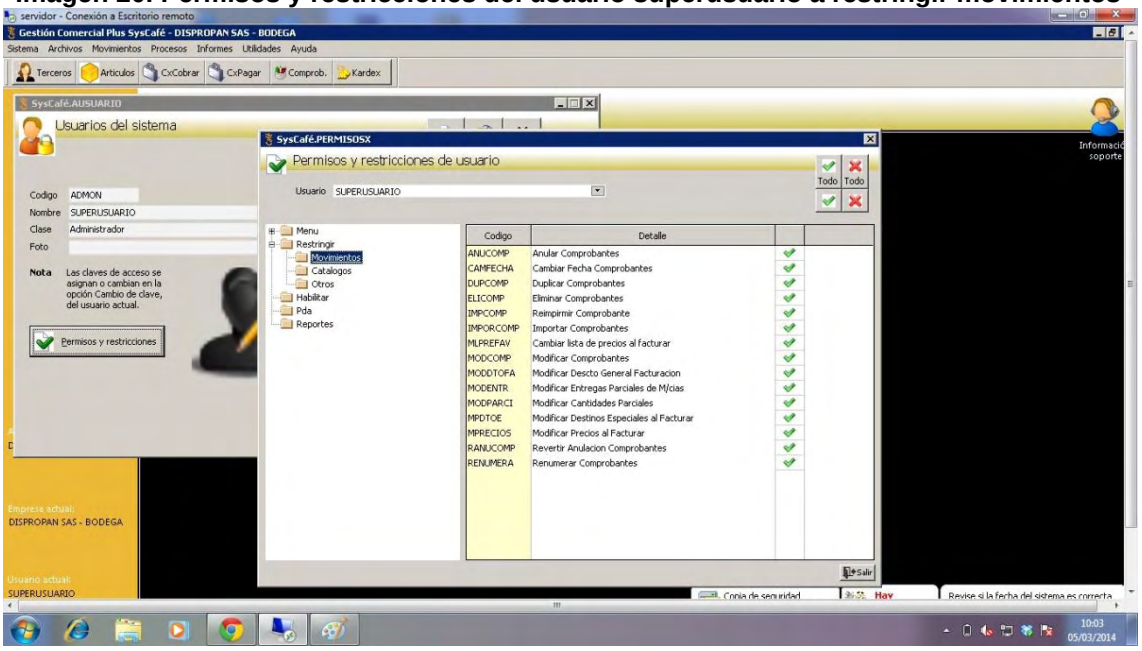


Imagen 21. Permisos y restricciones del usuario superusuario a restringir catálogos

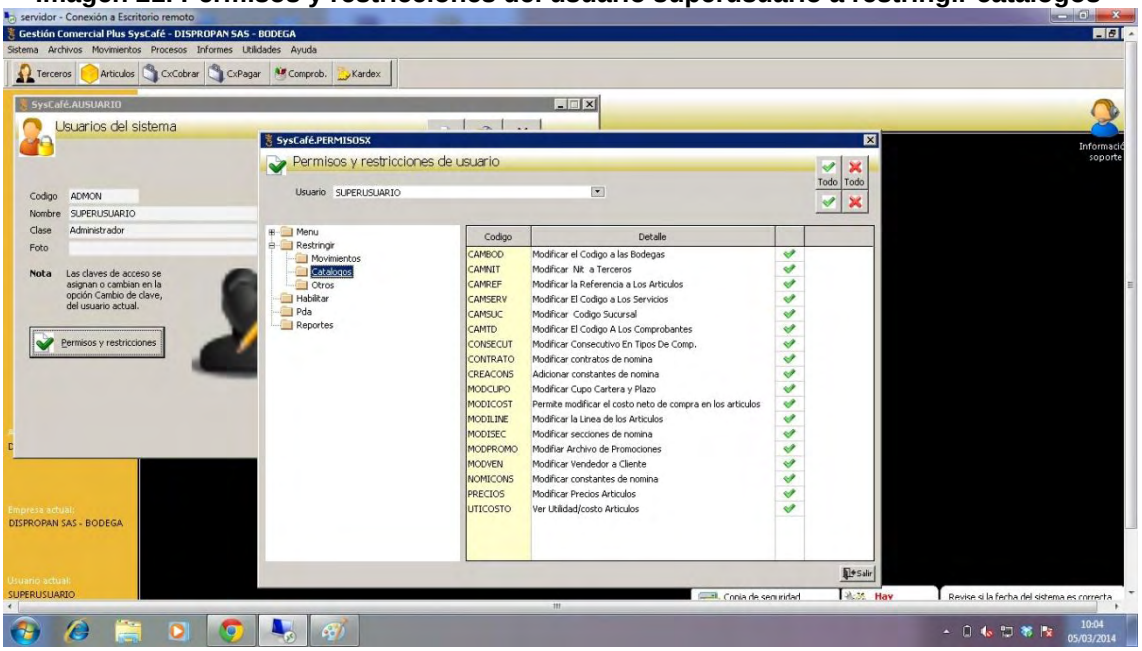


Imagen 22. Permisos y restricciones del usuario superusuario a restringir otros formatos

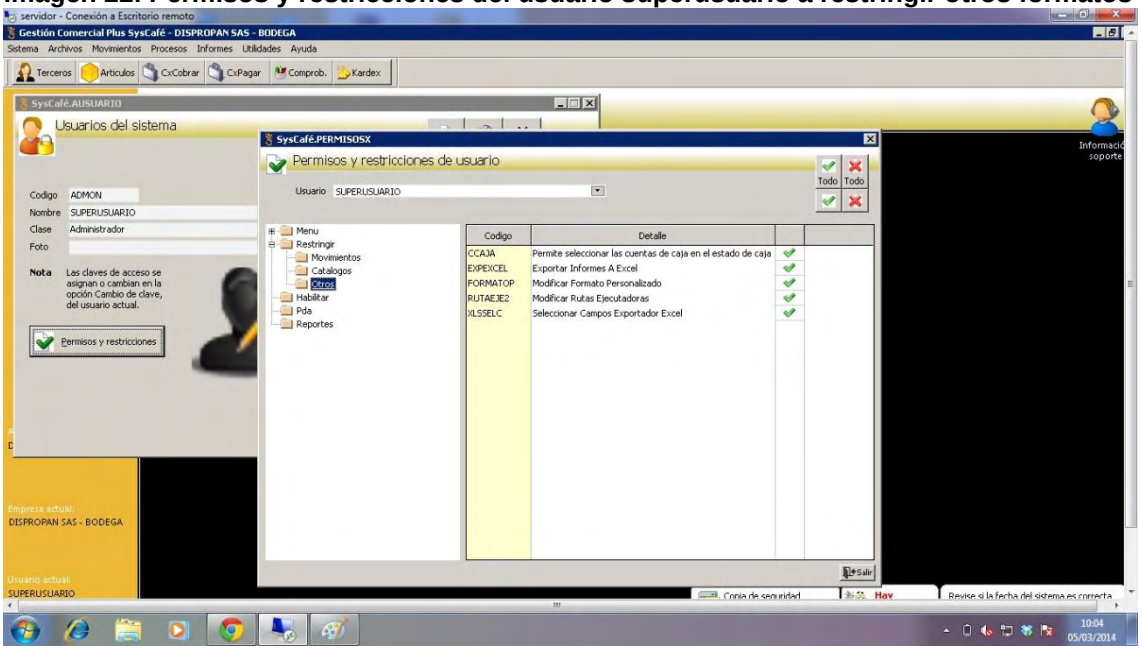


Imagen 23. Permisos y restricciones del usuario superusuario a habilitar formatos

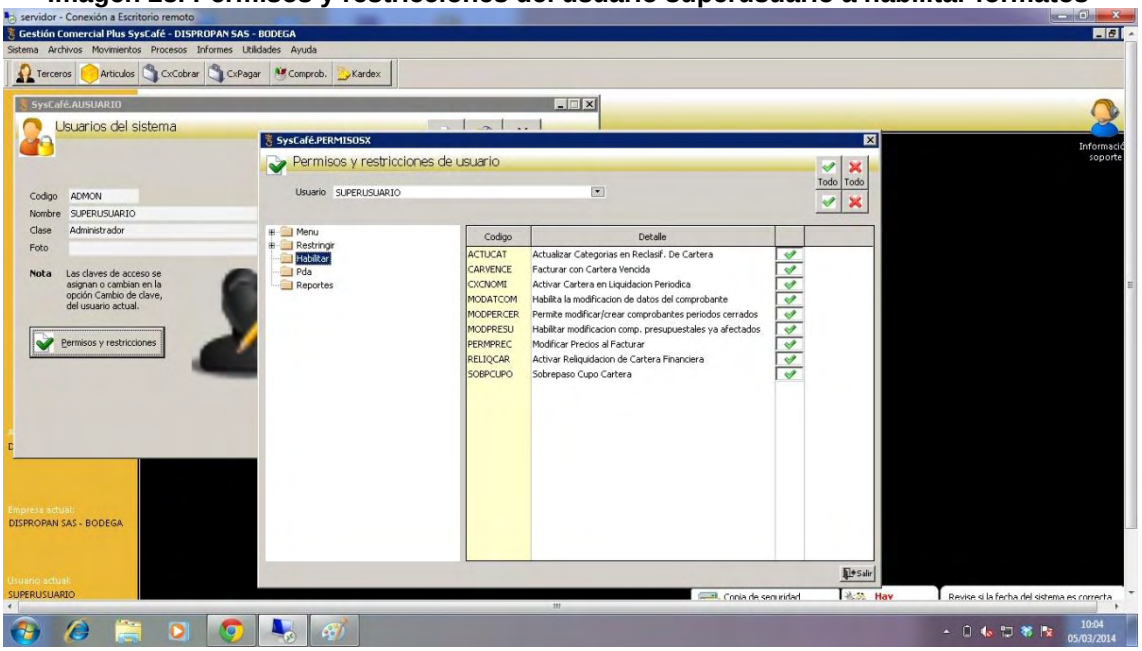


Imagen 24. Permisos y restricciones del usuario normal al sistema

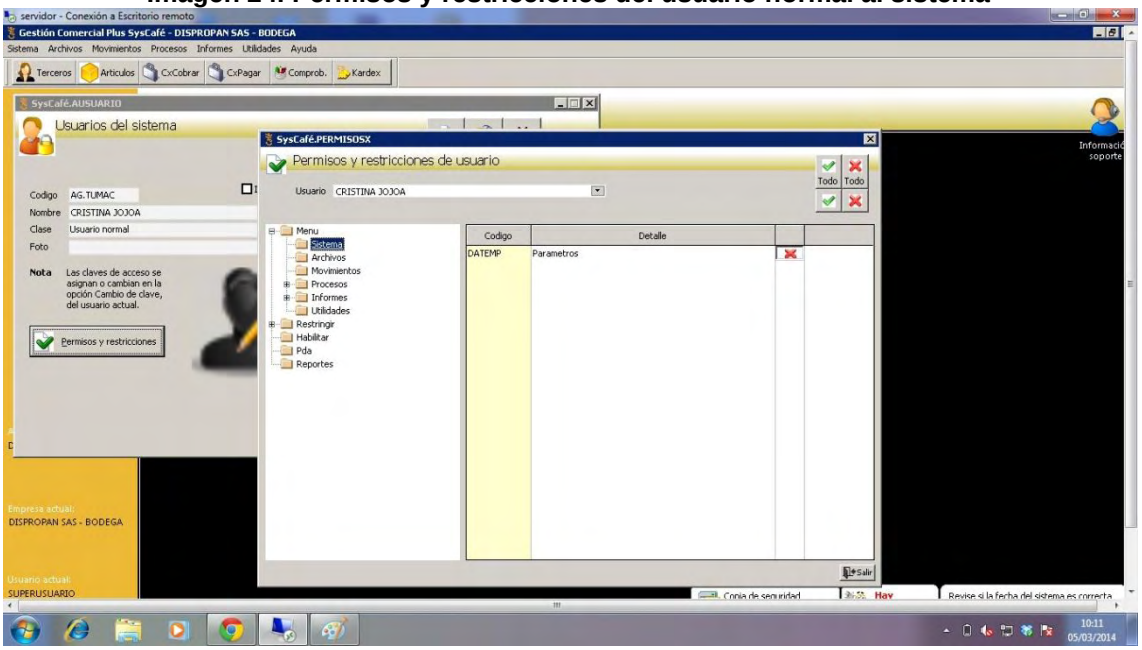


Imagen 25. Permisos y restricciones del usuario normal acceso a archivos

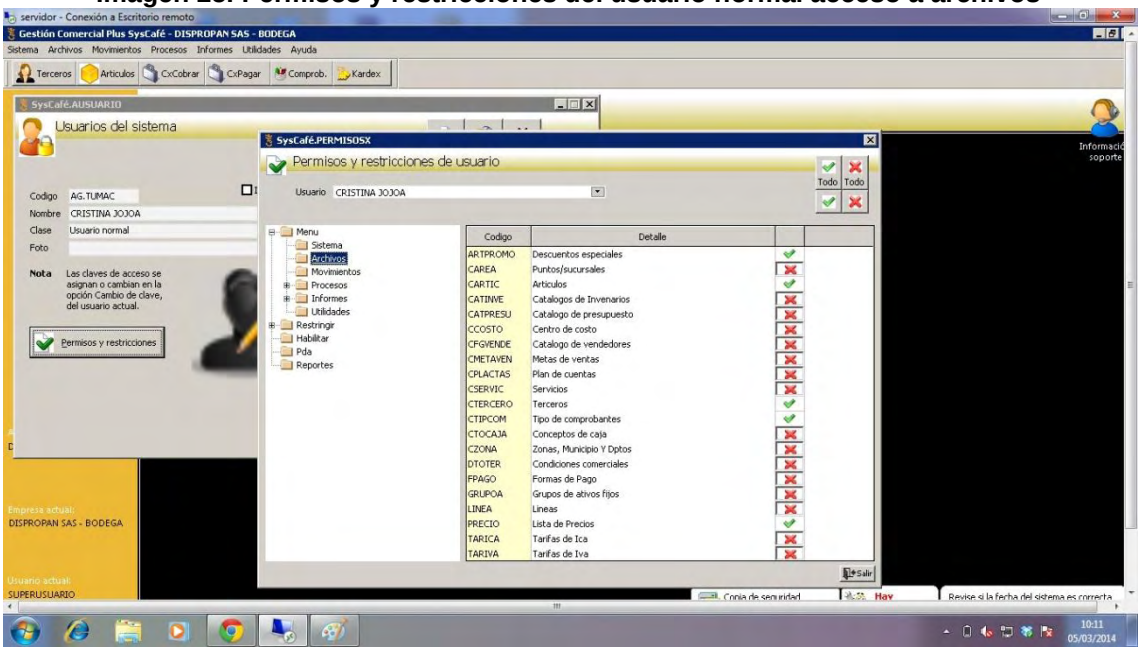


Imagen 26. Permisos y restricciones del usuario normal a movimientos

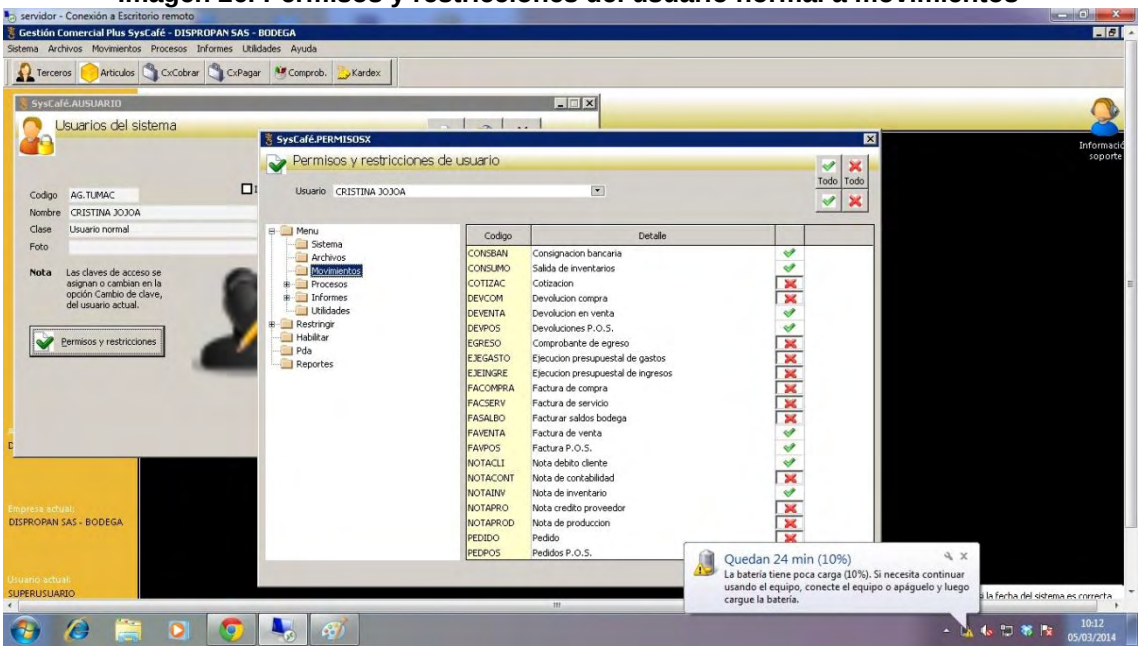


Imagen 27. Permisos y restricciones del usuario normal a procesos

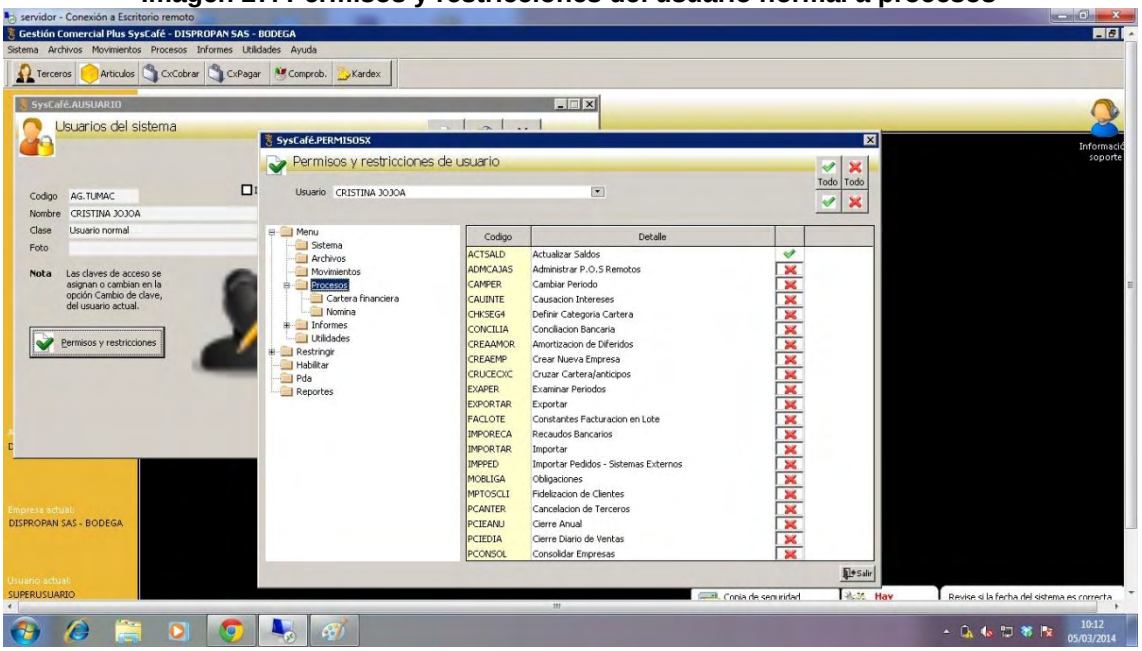


Imagen 28. Permisos y restricciones del usuario normal procesos de cartera financiera

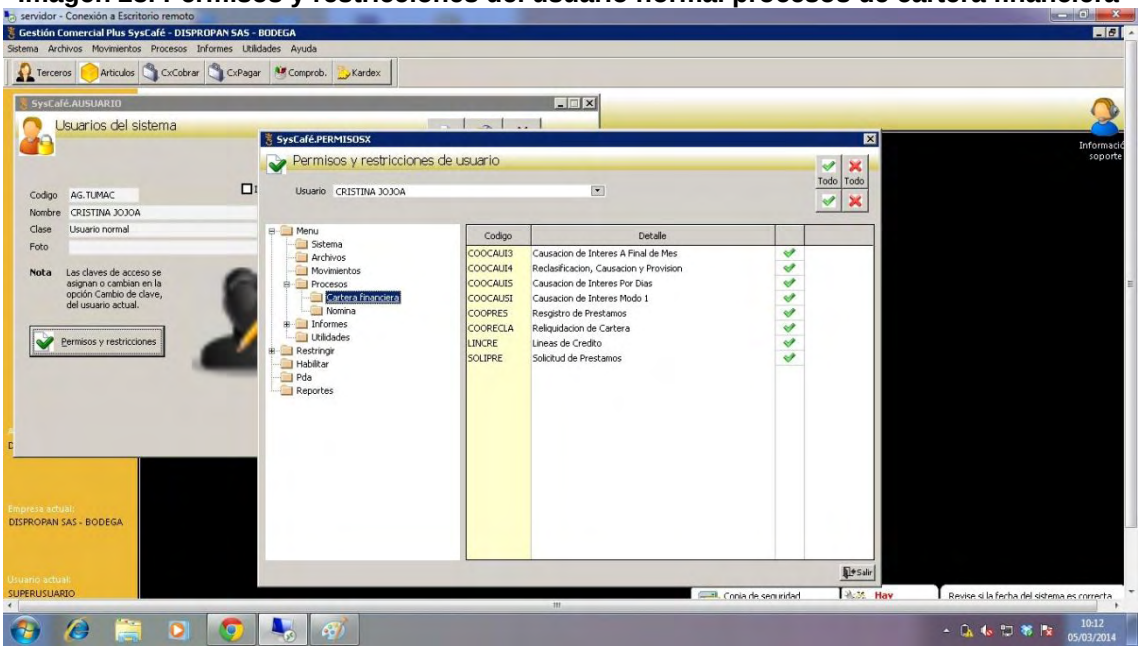


Imagen 29. Permisos y restricciones del usuario normal a procesos de nomina

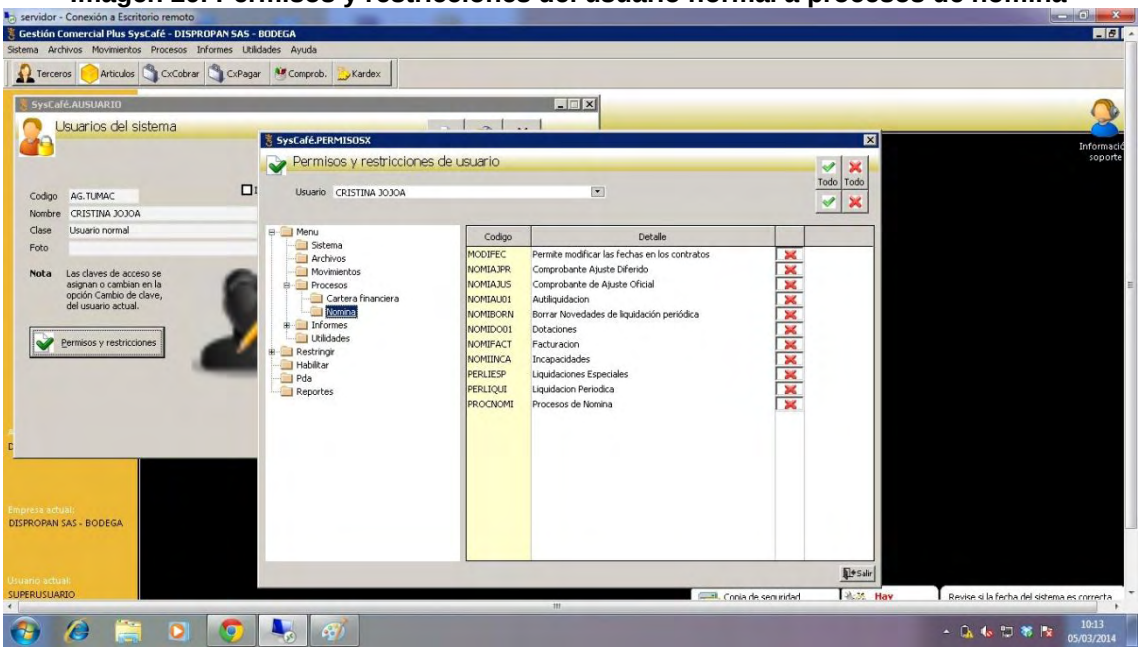


Imagen 30. Permisos y restricciones del usuario normal a informes de contabilidad

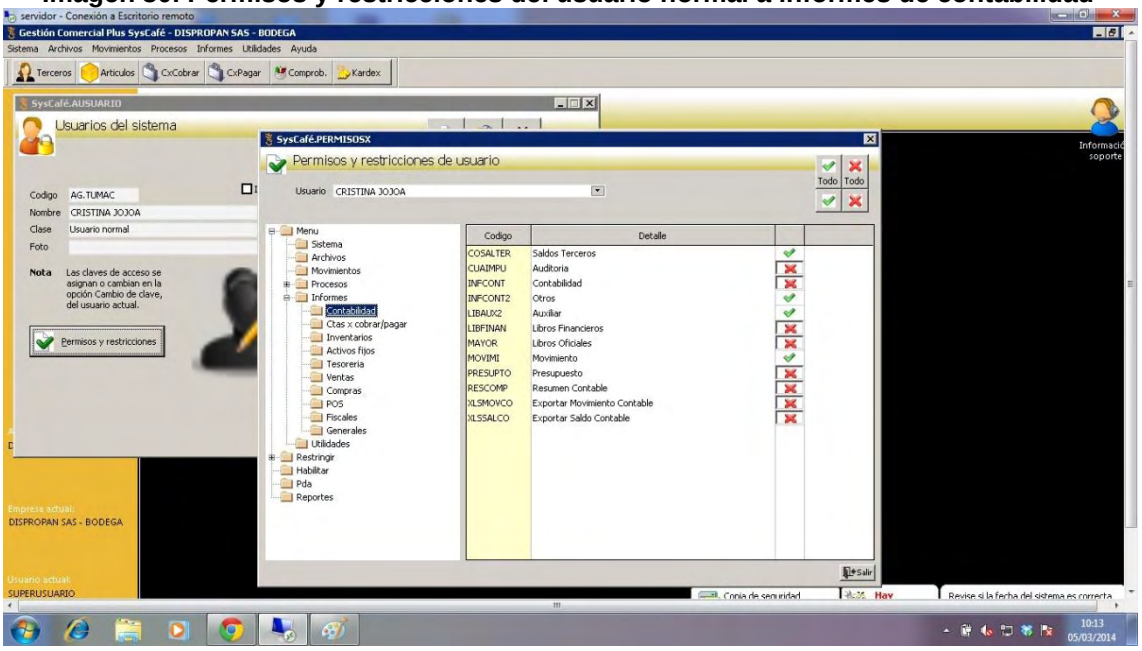


Imagen 31. Permisos y restricciones del usuario normal informes de ctas x cobrar

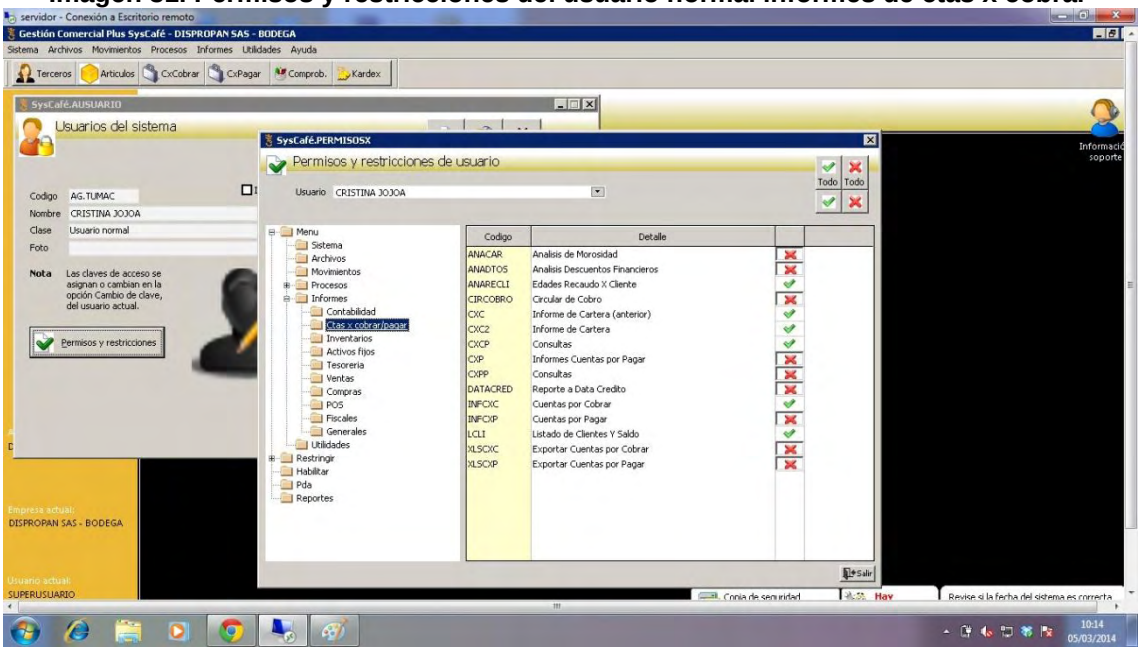


Imagen 32. Permisos y restricciones del usuario normal a informes de inventario

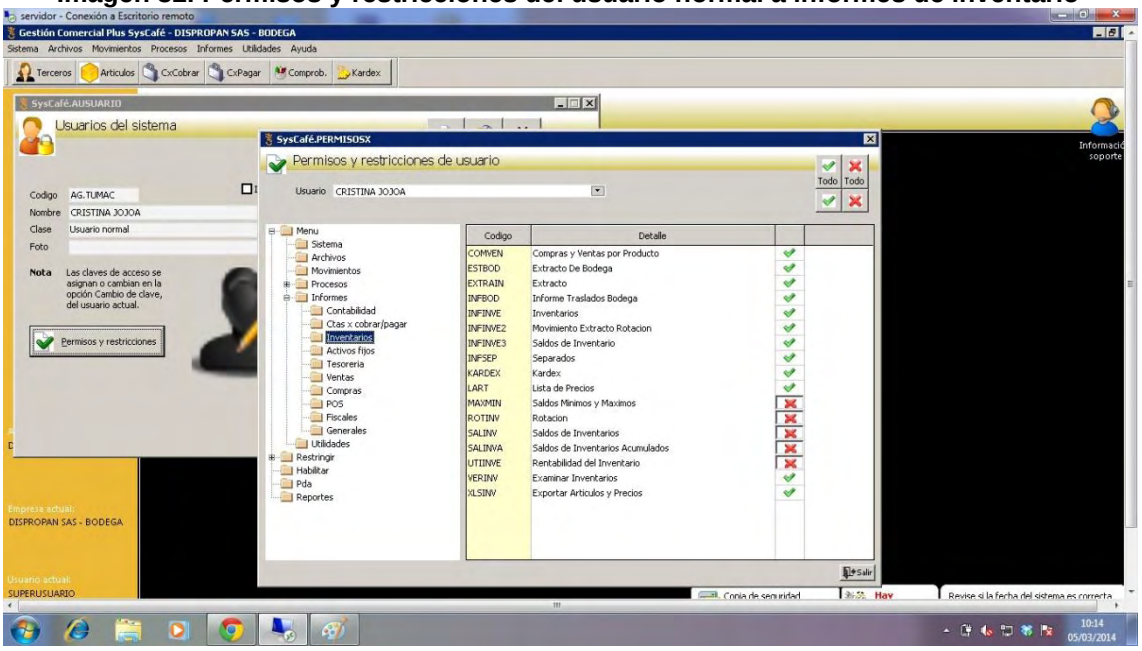


Imagen 33. Permisos y restricciones del usuario normal a informes de archivos fijos

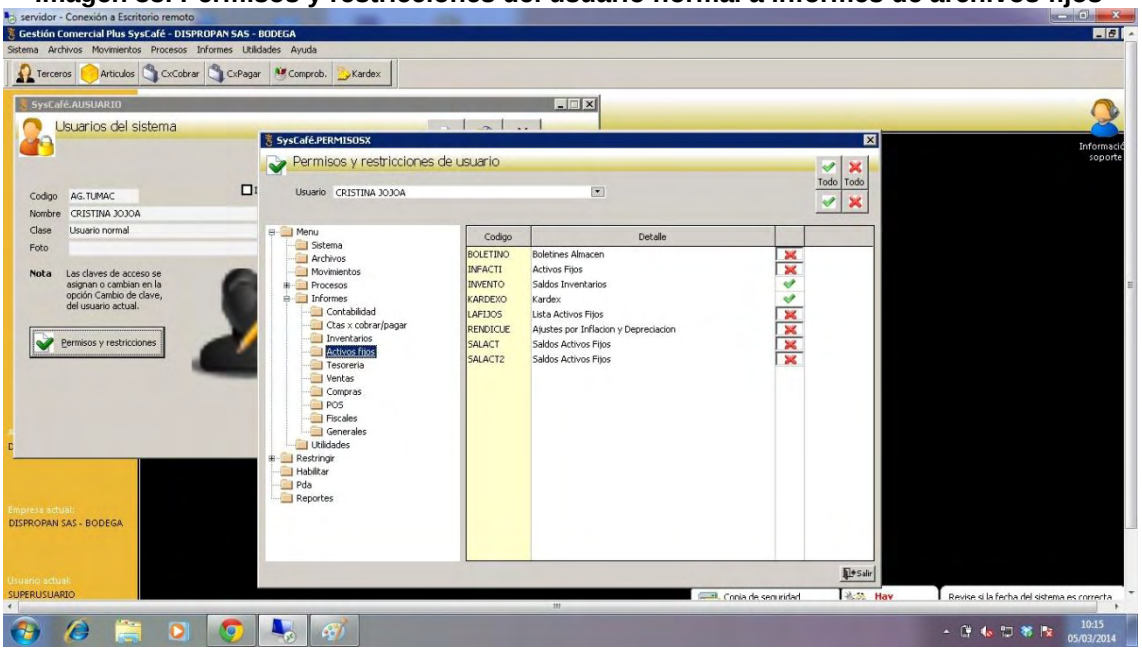


Imagen 34. Permisos y restricciones del usuario normal a informes de tesorería

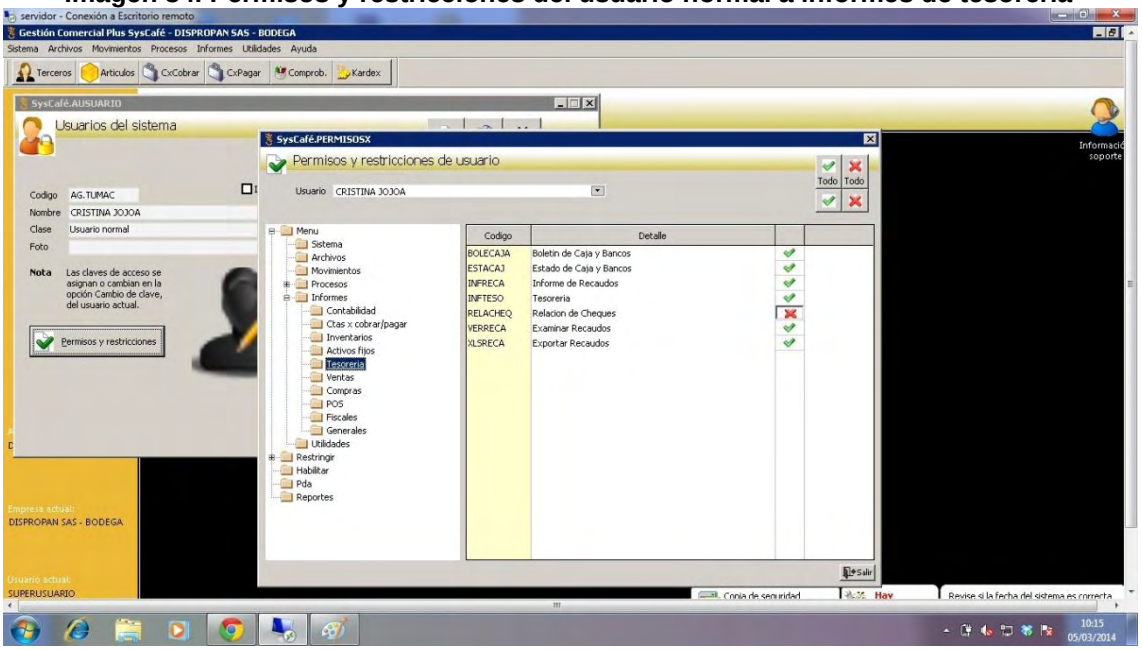


Imagen 35. Permisos y restricciones del usuario normal a informes de ventas

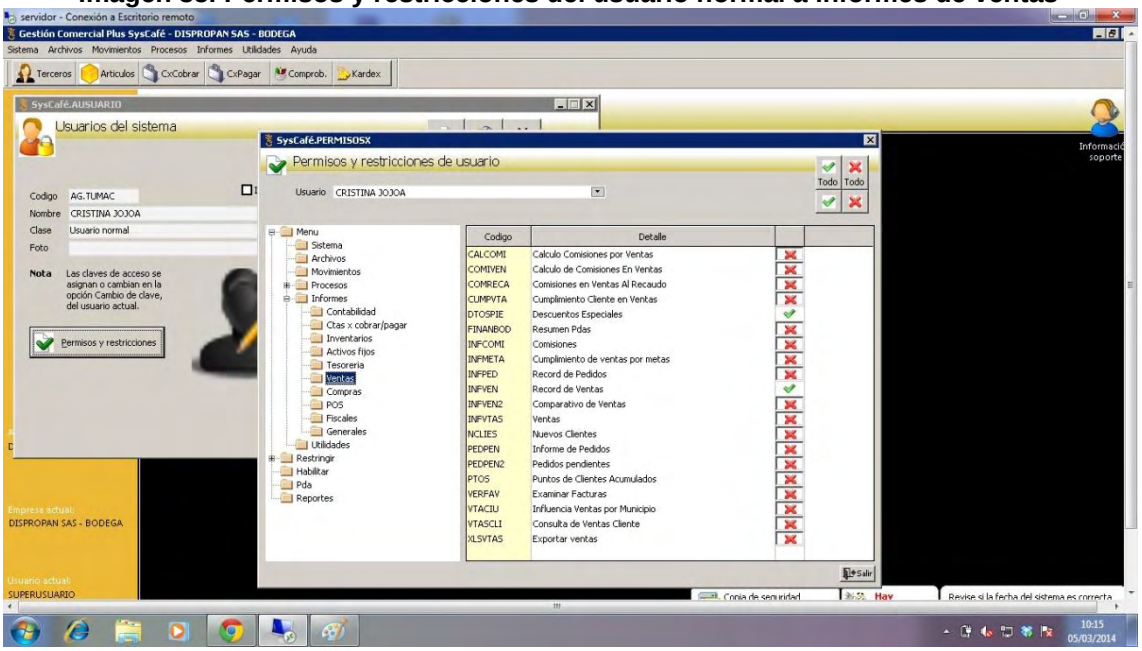


Imagen 36. Permisos y restricciones del usuario normal a informes compras

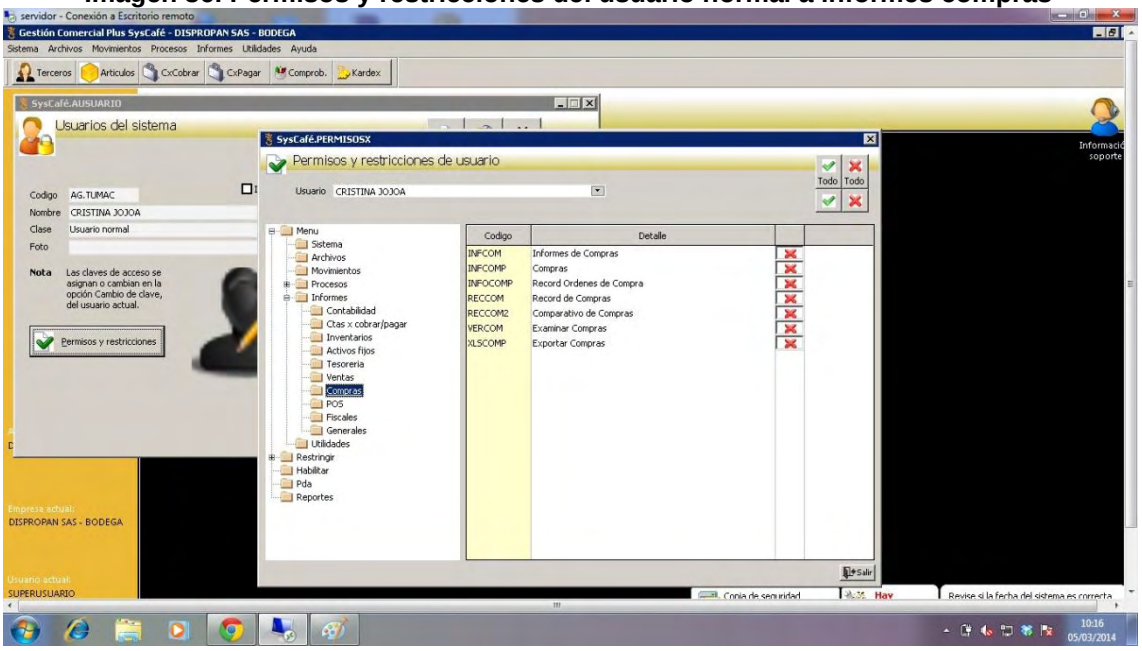


Imagen 37. Permisos y restricciones del usuario normal a informes fiscales

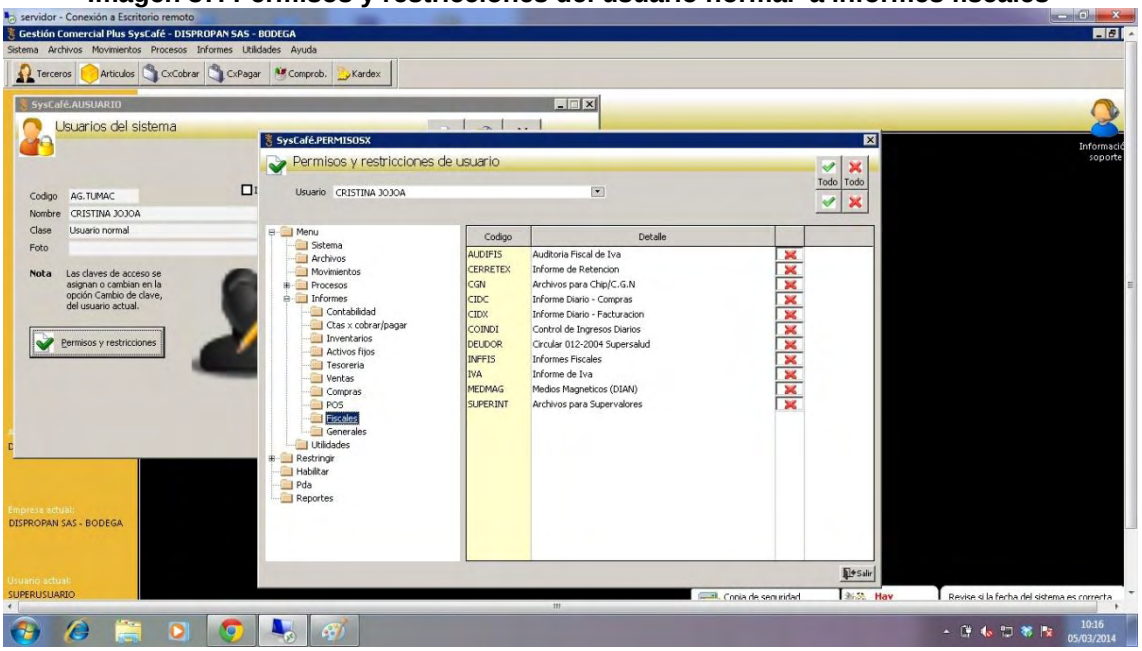


Imagen 38. Permisos y restricciones del usuario normal a informes generales

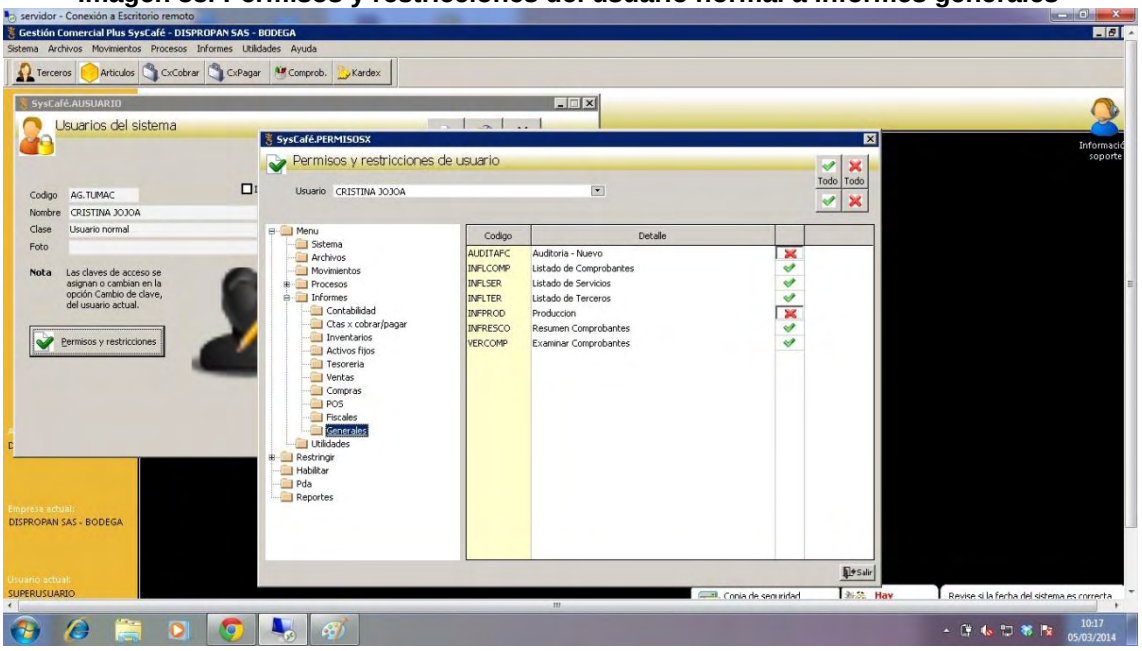


Imagen 39. Permisos y restricciones del usuario normal a utilidades del sistema

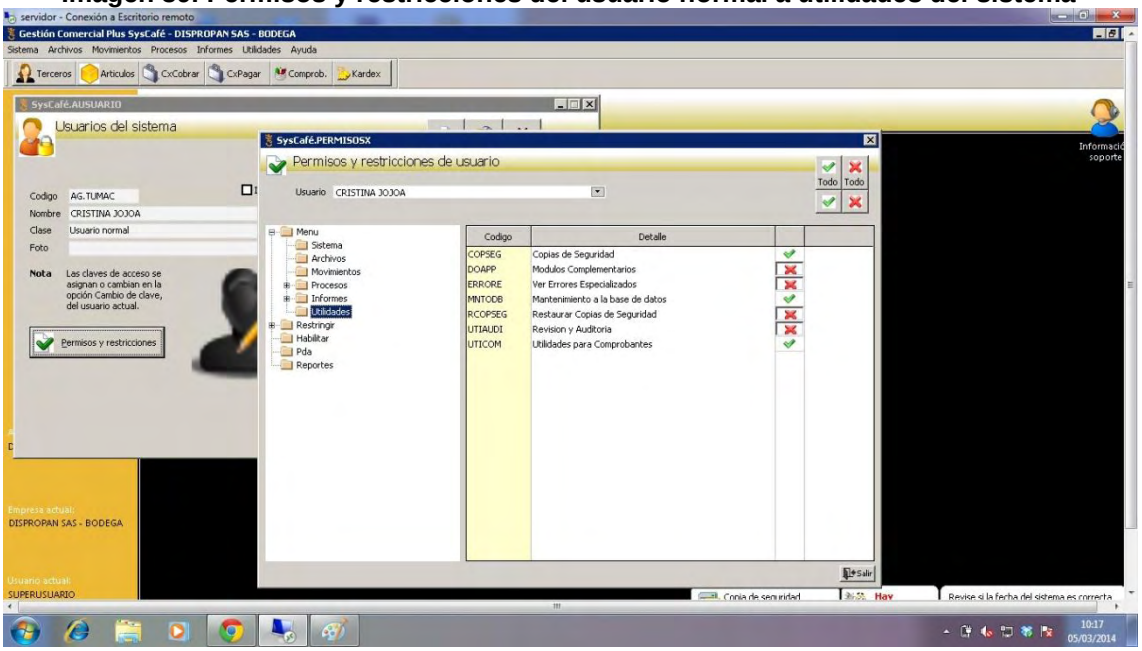


Imagen 40. Permisos y restricciones del usuario normal a restringir movimientos

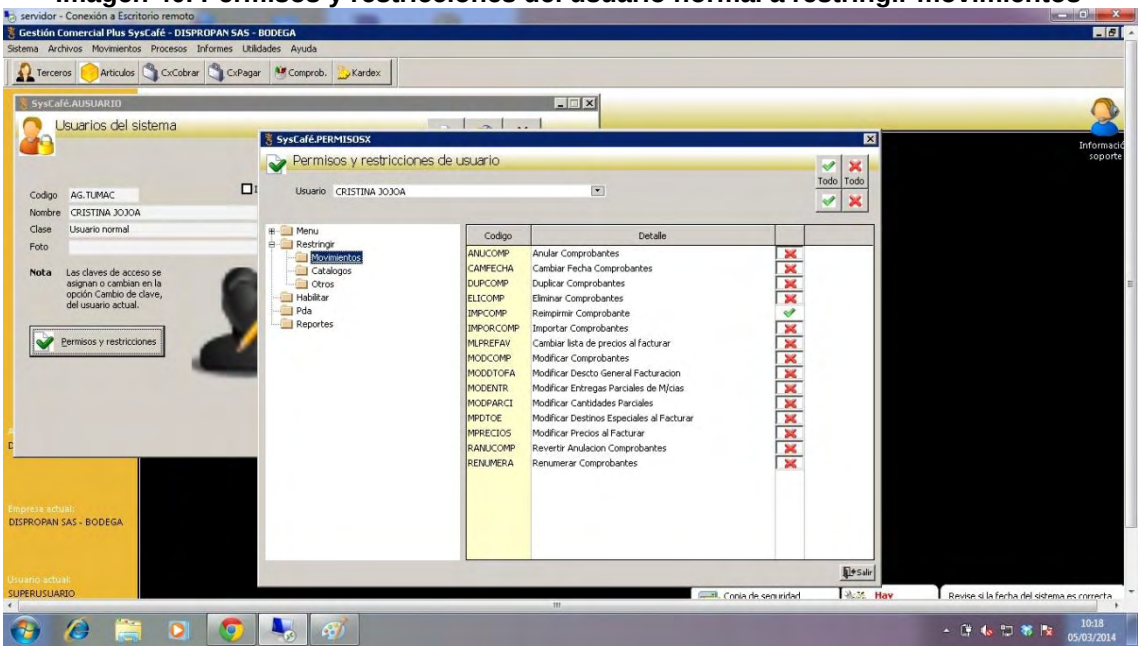


Imagen 41. Permisos y restricciones del usuario normal a restringir catálogos

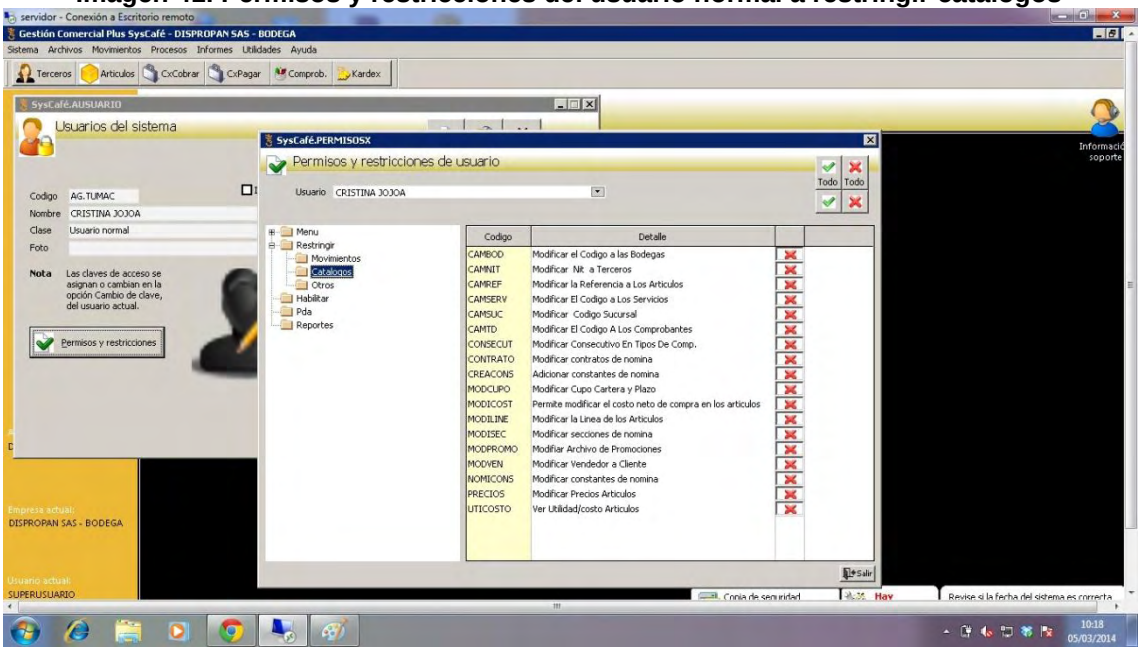


Imagen 42. Permisos y restricciones del usuario normal a restringir otros

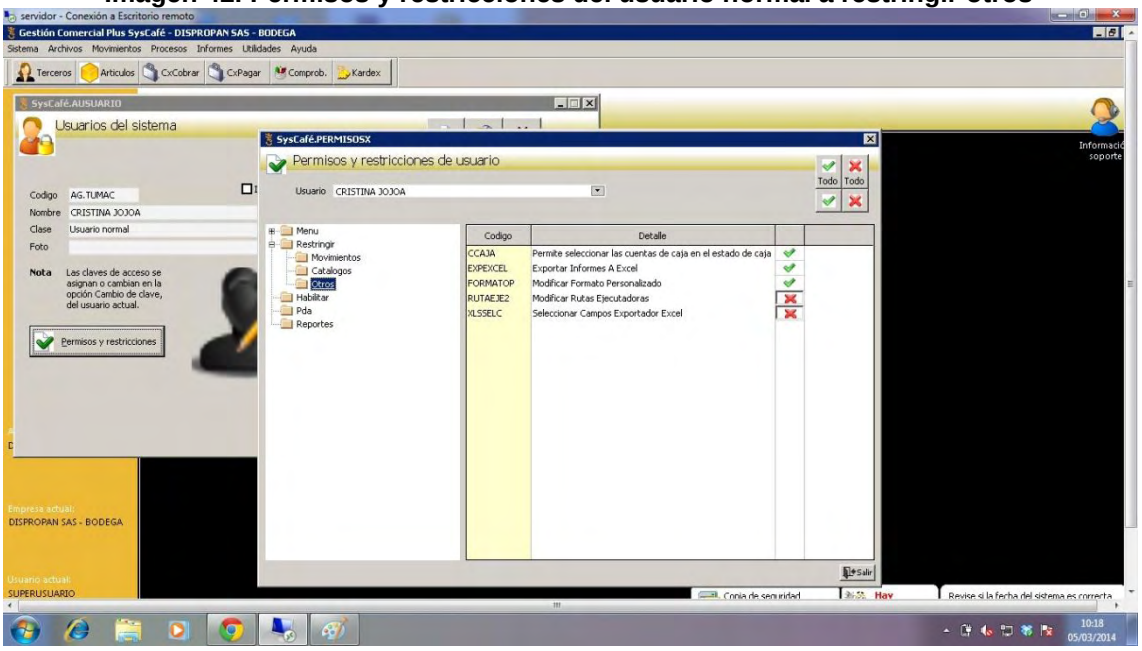
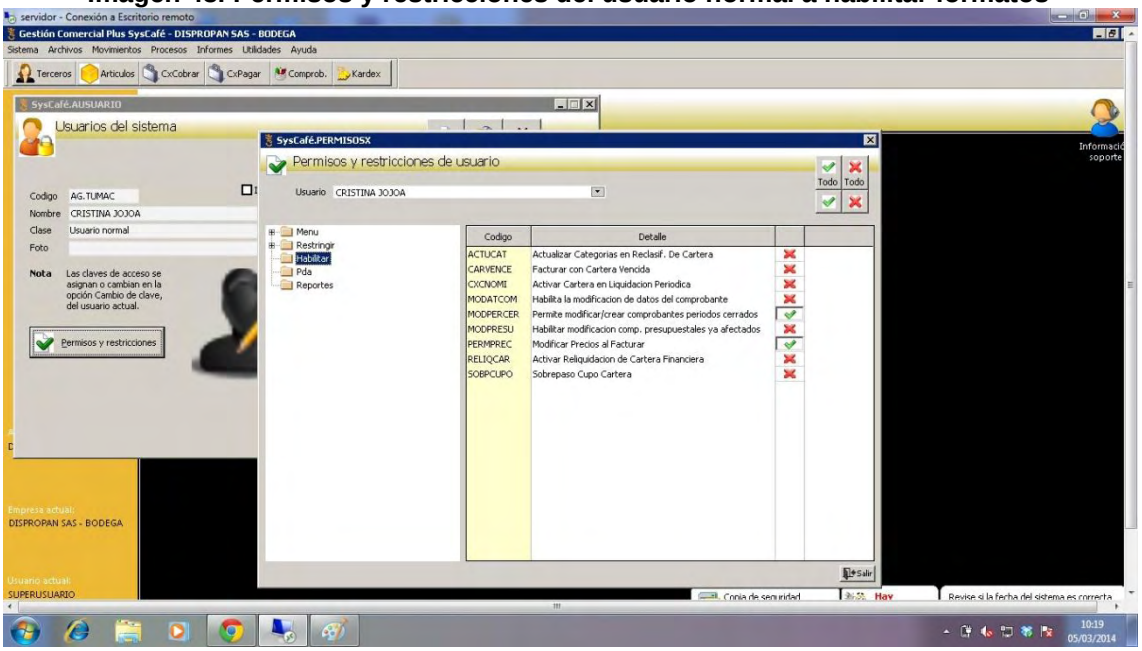


Imagen 43. Permisos y restricciones del usuario normal a habilitar formatos



	SOFTWARE GESTION SYSCAFE DISPROPAN	**REF** **SGDD_O6**

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA** 1 DE 16	
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds5)	

SOFTWARE GESTION SYSCAFE[14]

- Posee herramientas para el manejo contable, control de inventarios, tesorería, cuentas por cobrar y por pagar; generando informes de gran utilidad para el desarrollo de la labor administrativa y operativa.
- Contabilidad: Controlar para que los recursos sean administrados en forma eficaz, lo cual es posible con un proceso confiable de REGISTRO de transacciones;
  Informar a través de los estados financieros los efectos de las operaciones practicadas, observando y evaluando el comportamiento de la entidad dentro de un periodo de tiempo.
  A través de este proceso se pueden realizar los registros contables para obtener cualquier tipo de reporte, sea fiscal, contable o financiero además de poder exportarlos a Microsoft Excel. De fácil manejo e interpretación.
- Facturación y ventas: Proceso para el manejo de facturación de Ventas de Bienes y servicios.
- Tesorería: Permite la eficaz y segura administración de documentos comerciales y facilitan su auditoría a través de informes.
- Cuentas por pagar y por cobrar: Solución para el manejo eficiente del recaudo, control de cartera así como el manejo de proveedores y pagos.
- Inventarios: La base de toda empresa comercial es la compra y venta de bienes; de aquí la importancia del manejo del inventario por parte de la misma. Este proceso permitirá a la empresa mantener el control oportuno, así como también conocer al final del periodo contable un estado confiable de la situación económica de la empresa. Manejo completo, eficiente y confiable de los artículos

[14] www.syscafe.com.co/productos/gestion-comercial-cafe.html

3.4 VISION DE LOS MODULOS DEL SOFTWARE

Imagen 44. Ingreso al sistema – usuario - empresa

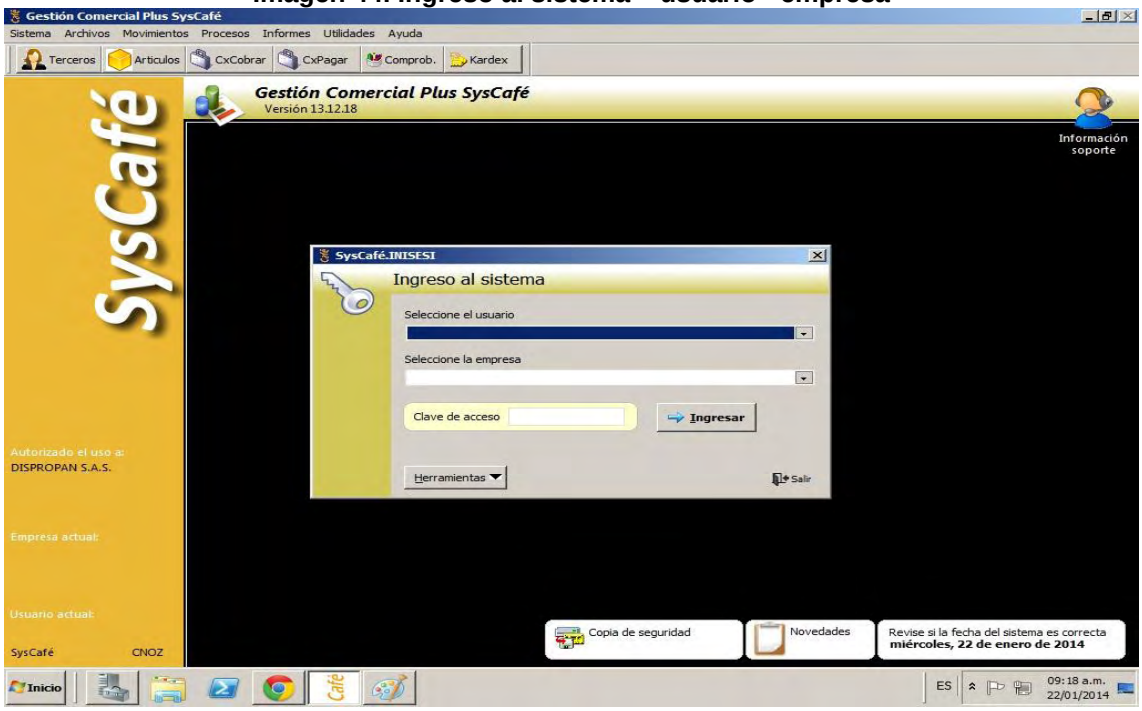


Imagen 45. Ingreso al sistema – seleccionar usuario

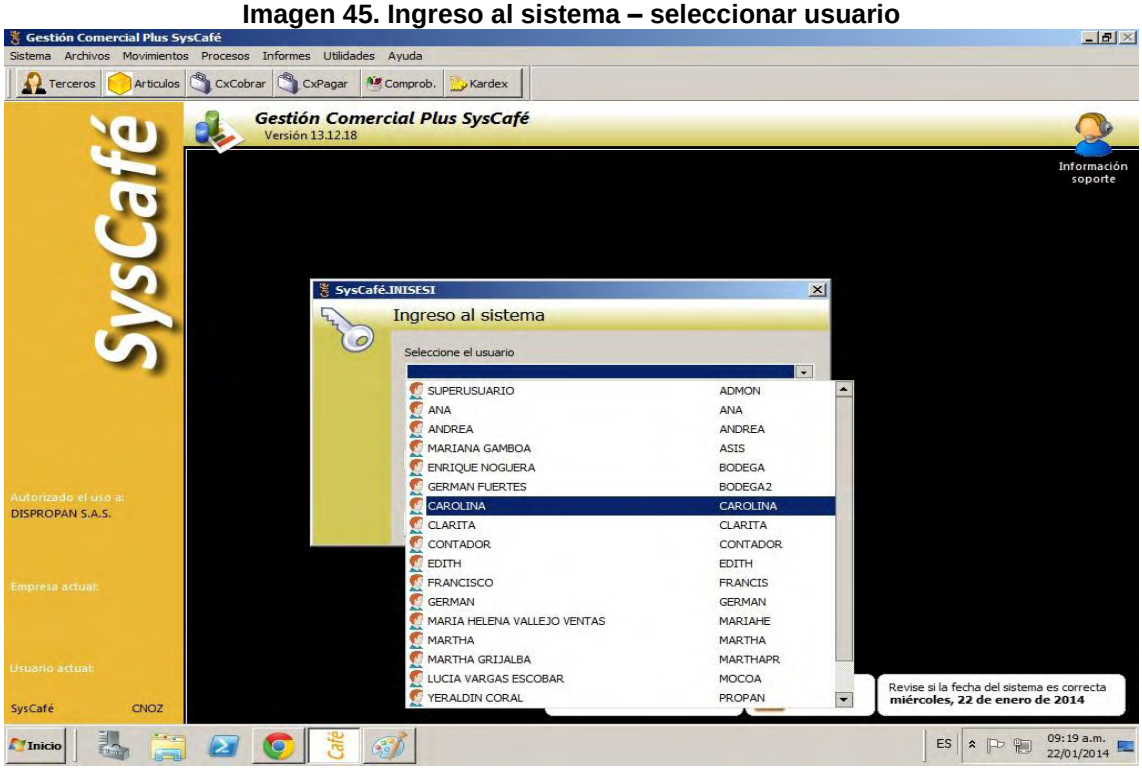


Imagen 46. Ingreso al sistema – seleccione la empresa

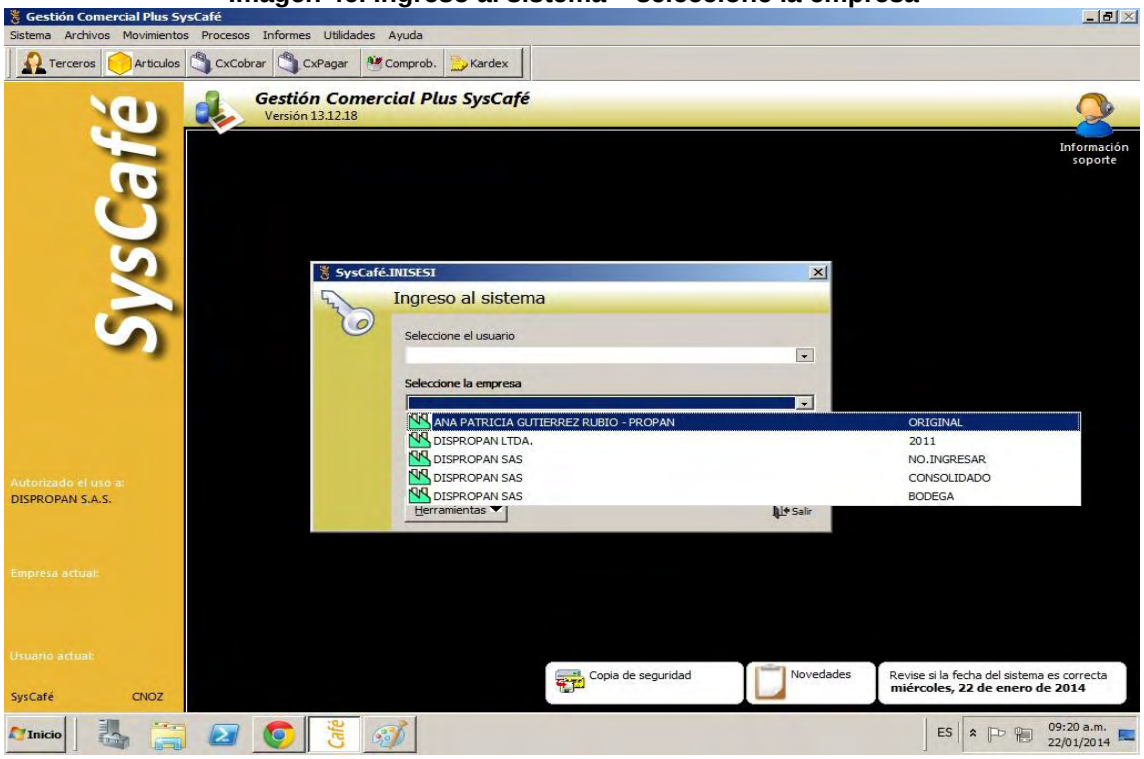


Imagen 47. Pantalla principal del software

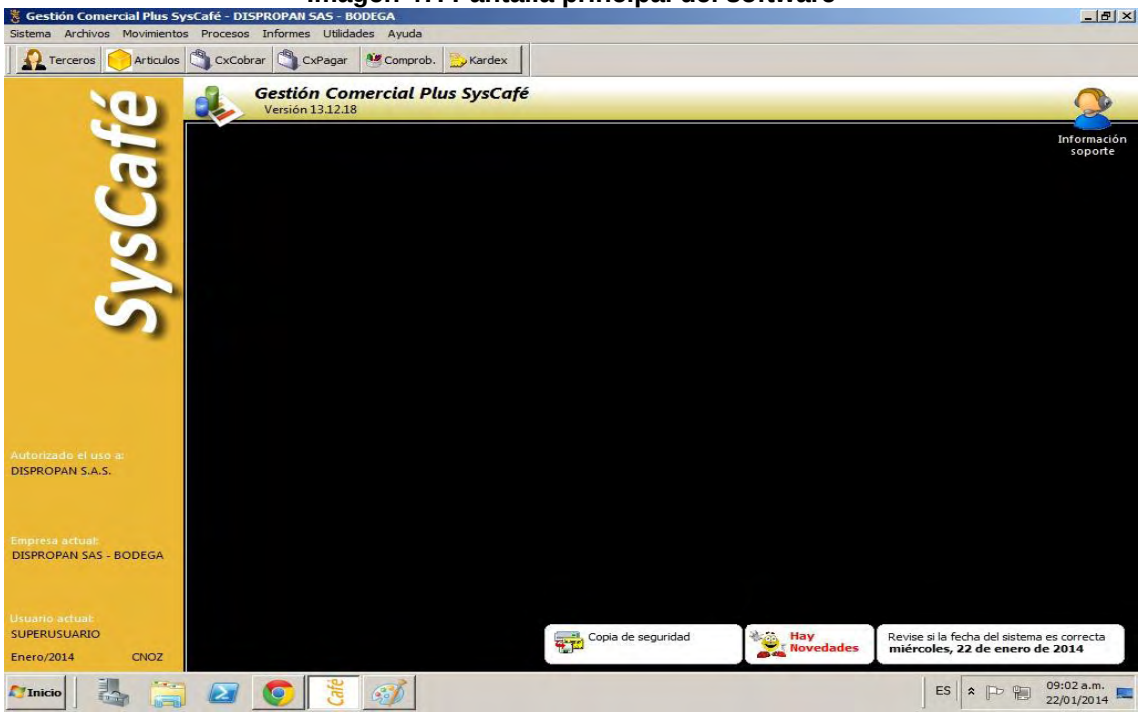


Imagen 48. Información catálogo de terceros

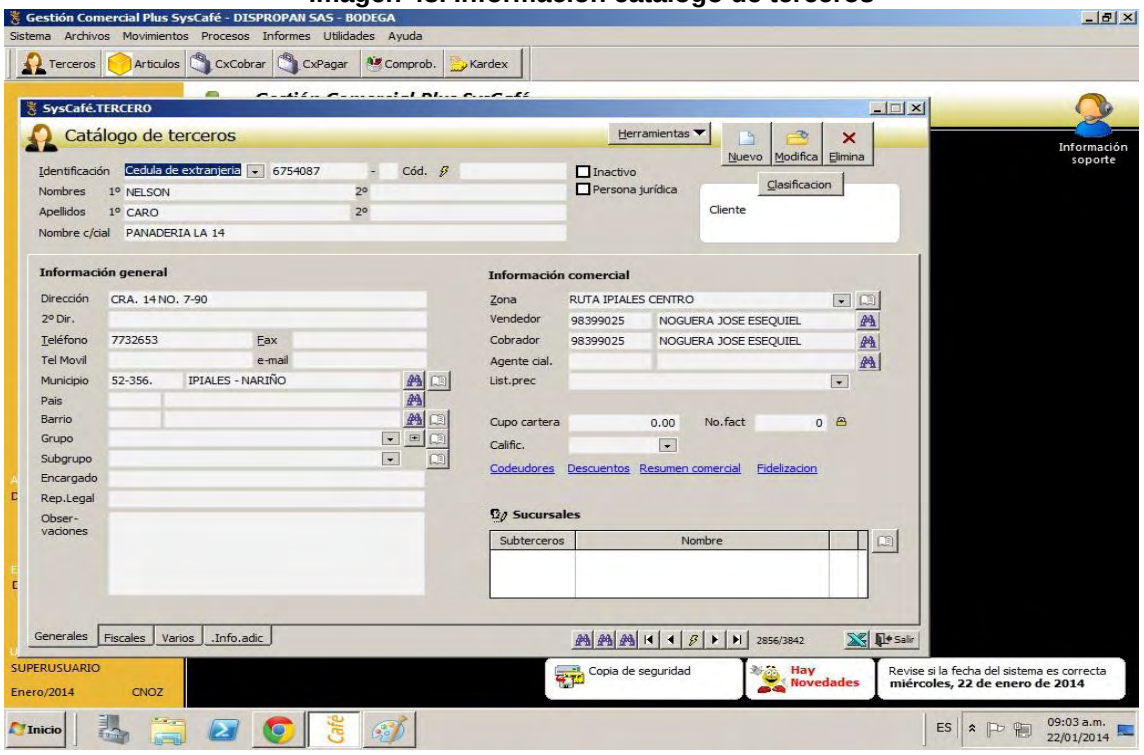


Imagen 49. Información catálogo de terceros – clasificación tributaria

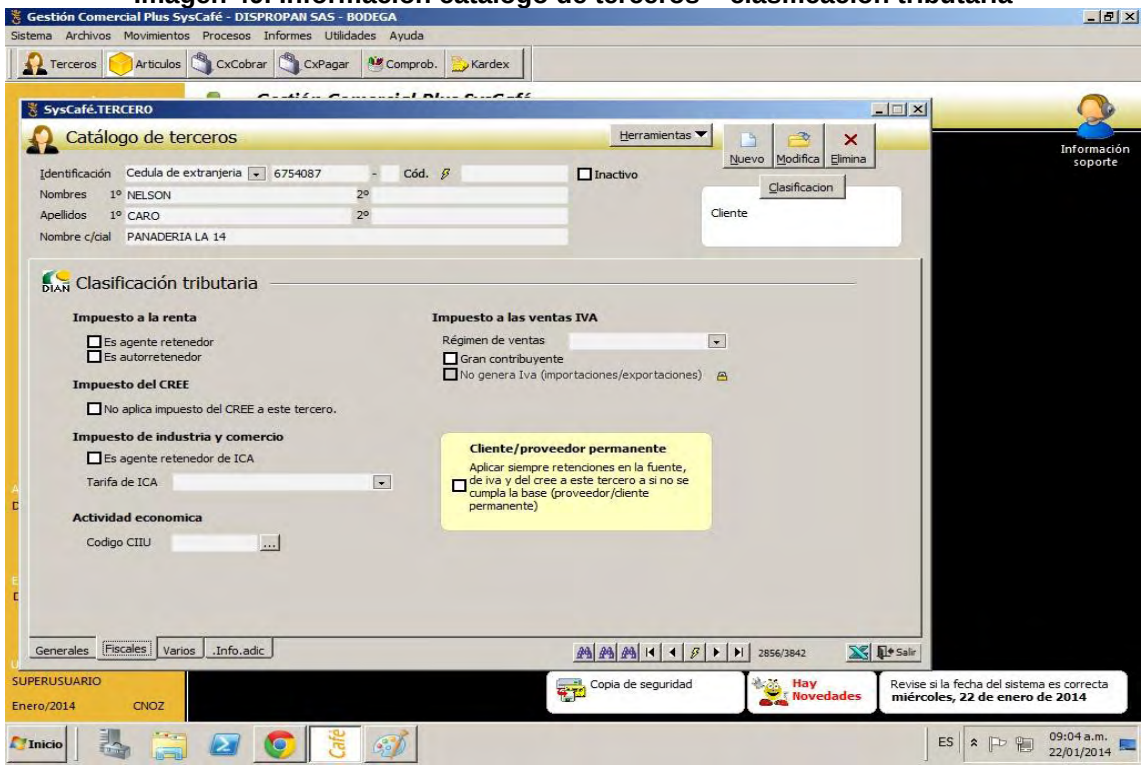


Imagen 50. Información catálogo de terceros – datos varios

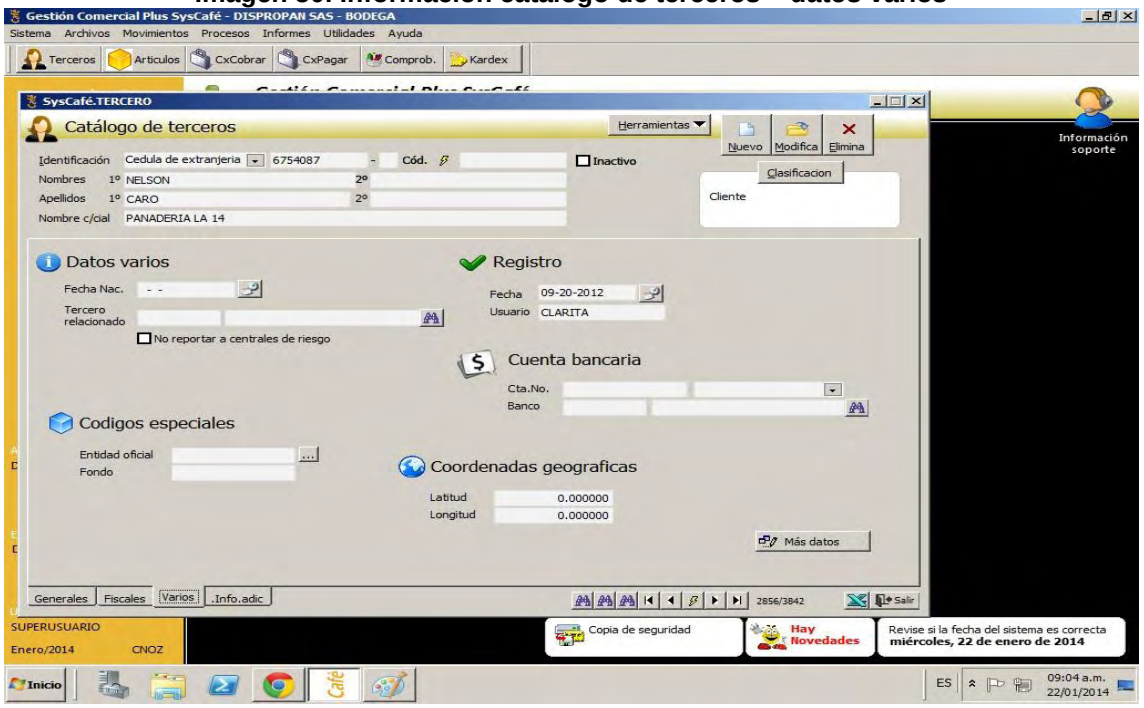


Imagen 51. Información catálogo de terceros – información adicional

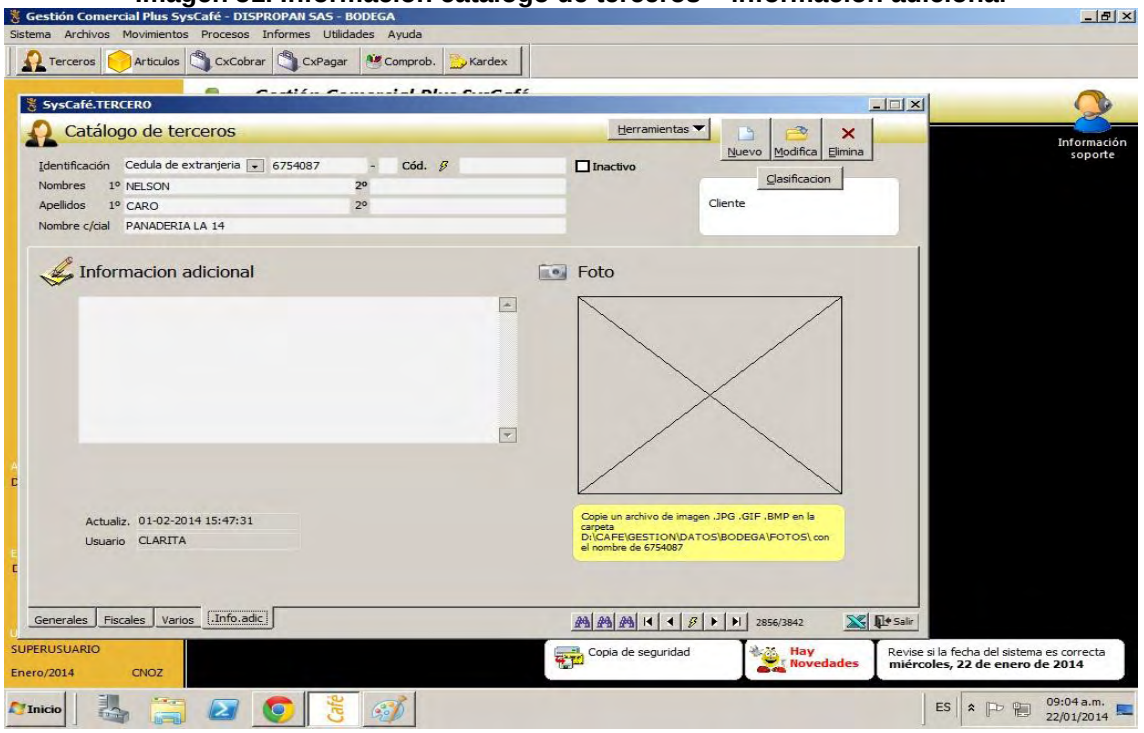


Imagen 52. Información catálogo artículos

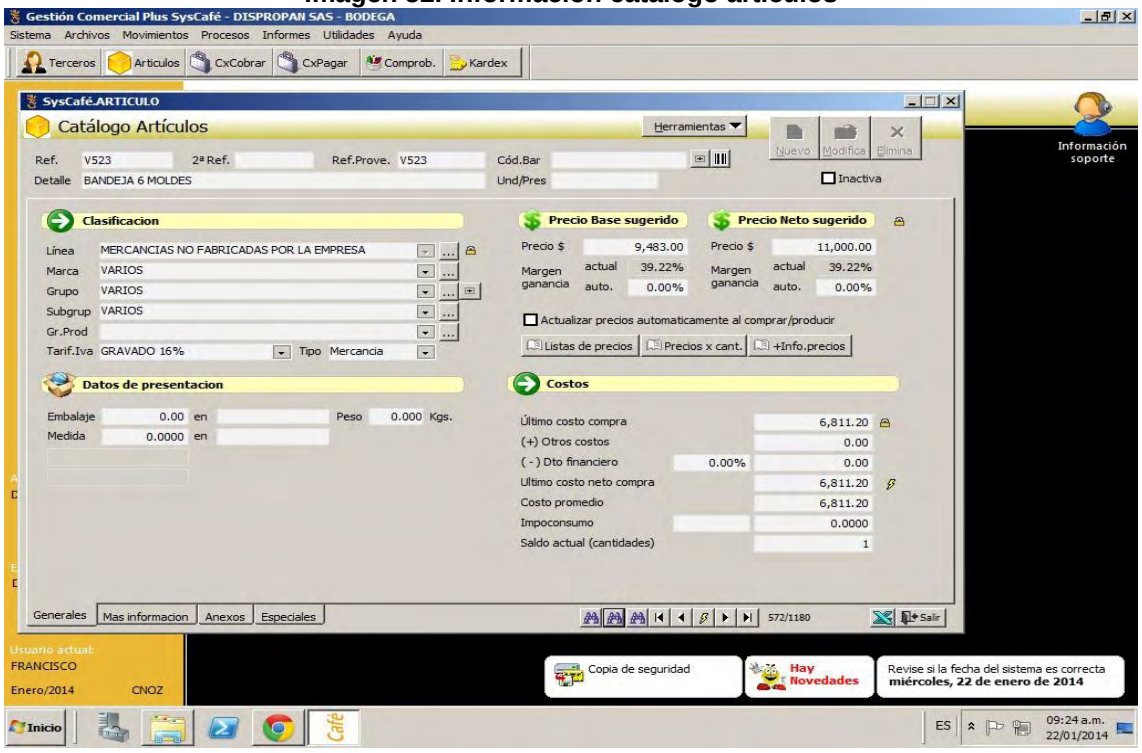


Imagen 53. Información catálogo artículos - proveedores

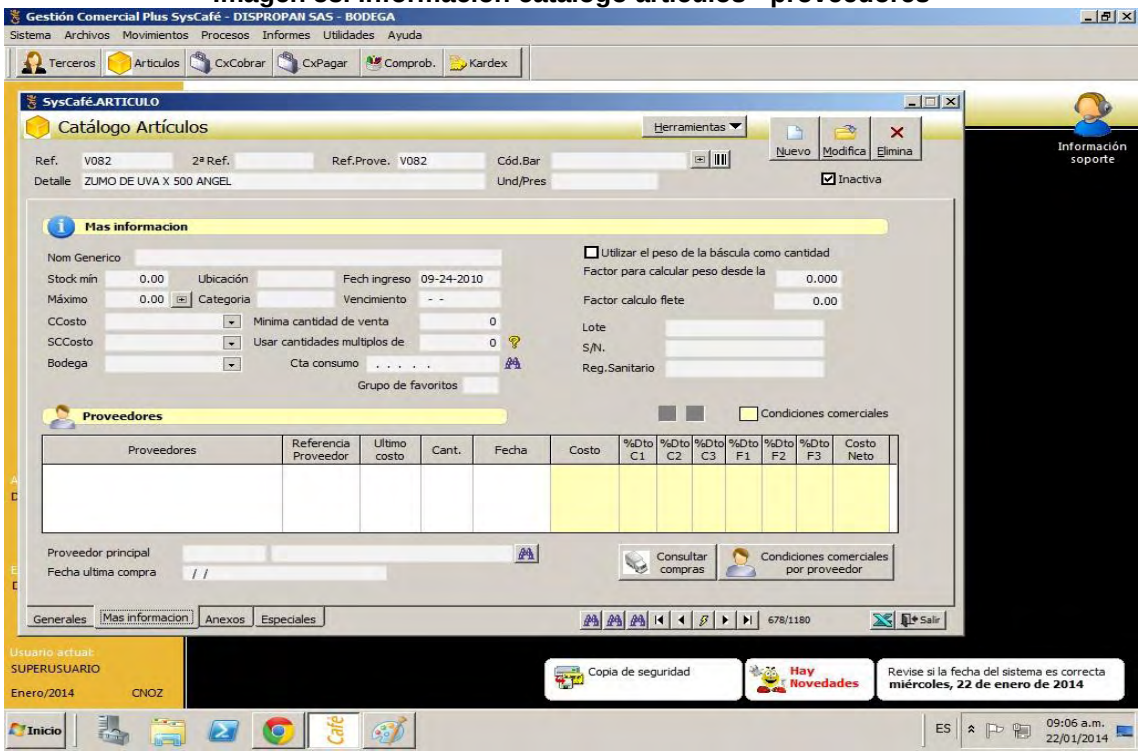


Imagen 54. Información de catálogo artículos - anexos

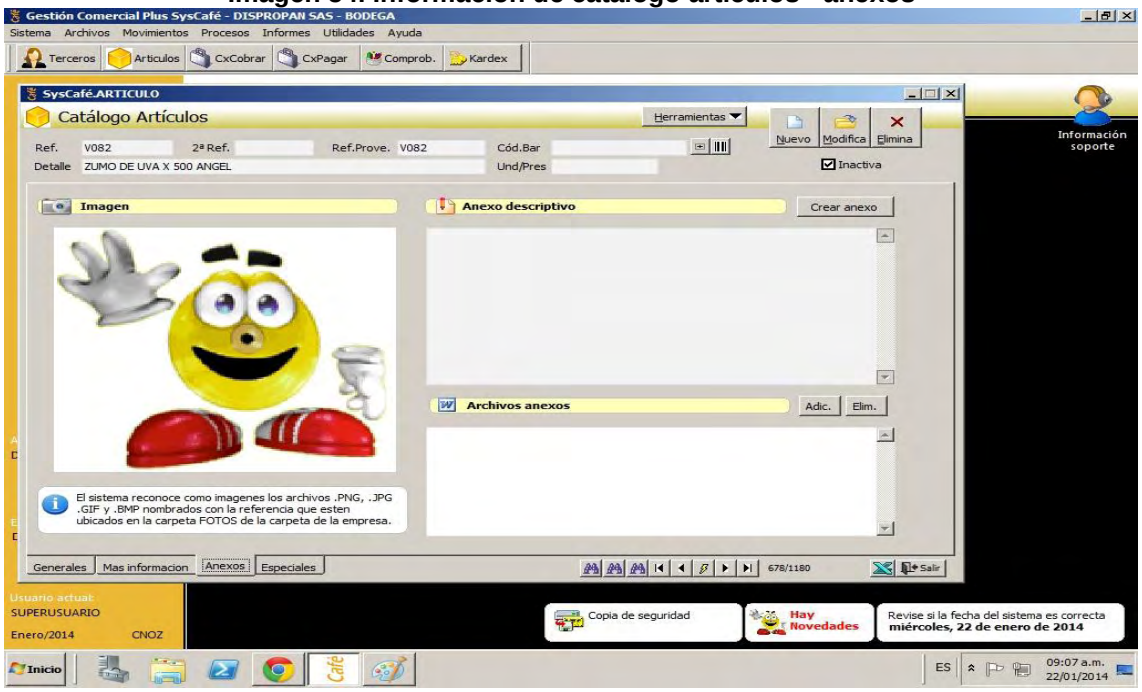


Imagen 55. Información del catálogo artículos - herramientas

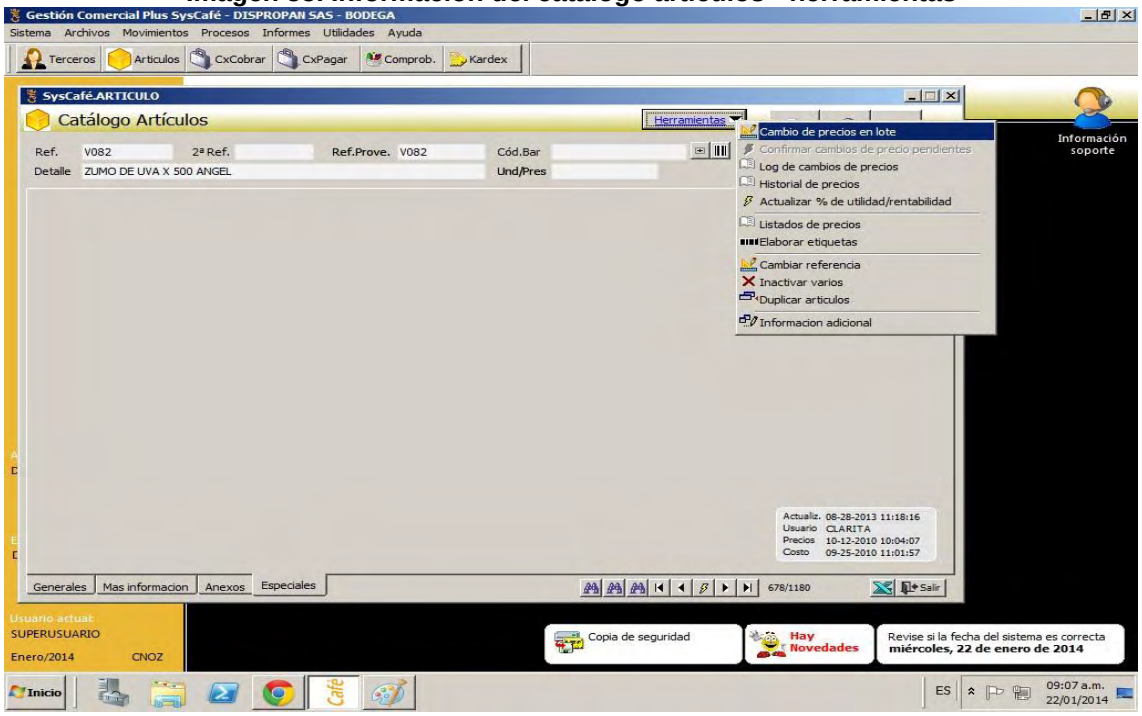


Imagen 56. Información módulos cuentas x cobrar

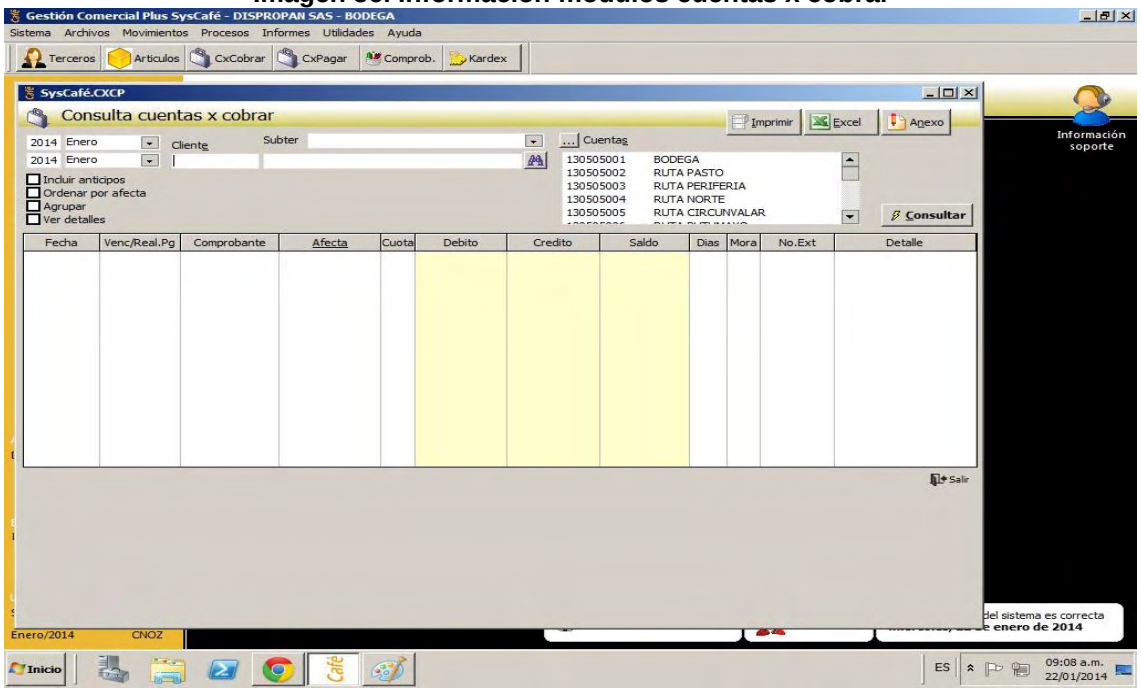


Imagen 57. Información módulos cuentas x pagar

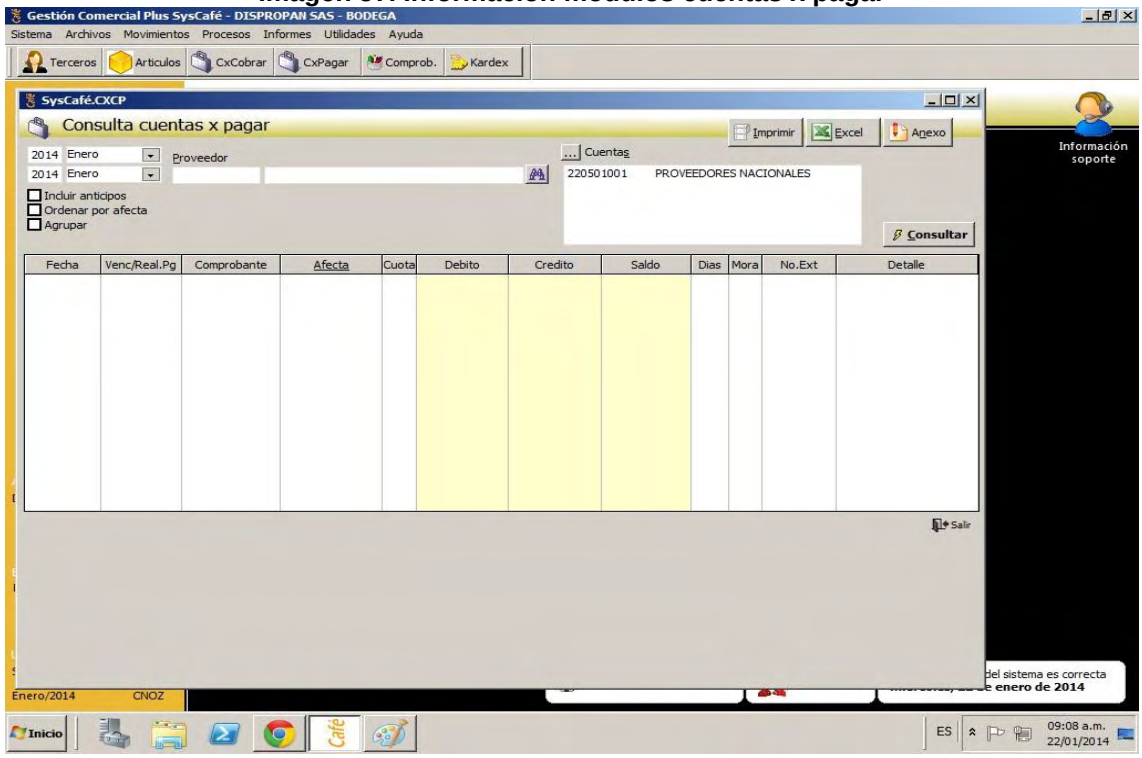


Imagen 58. Información utilidades en comprobantes

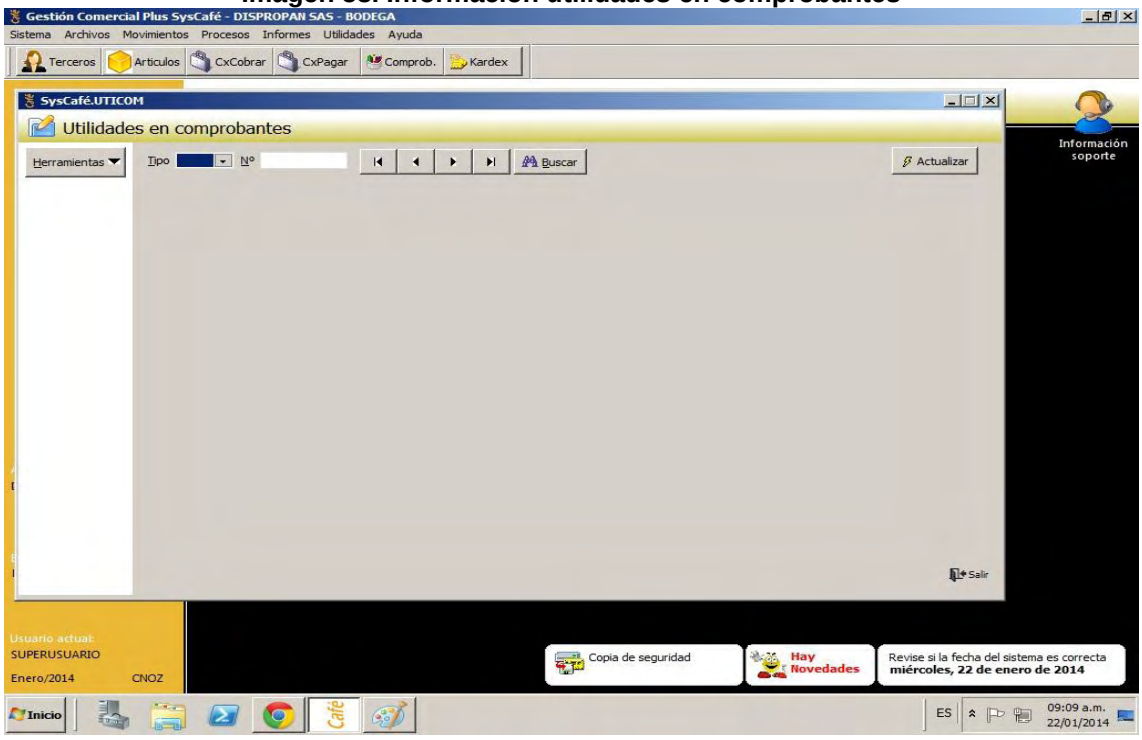


Imagen 59. Información kardex

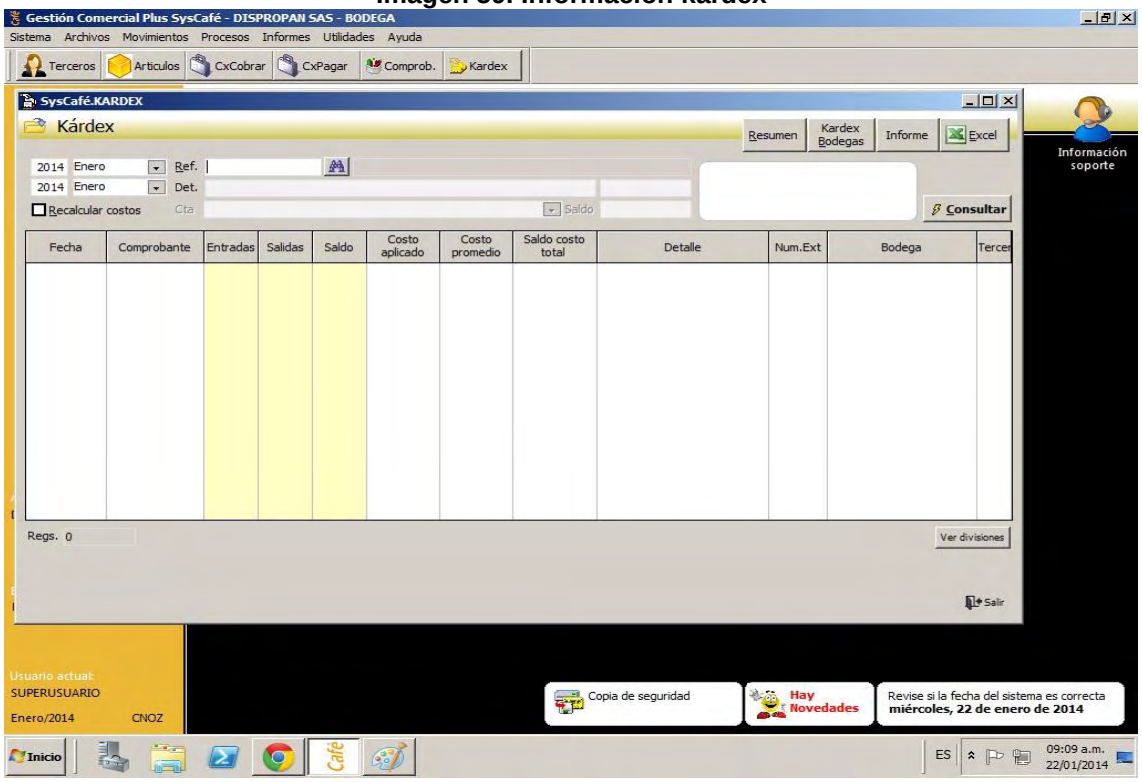


Imagen 60. Información resúmenes kardex

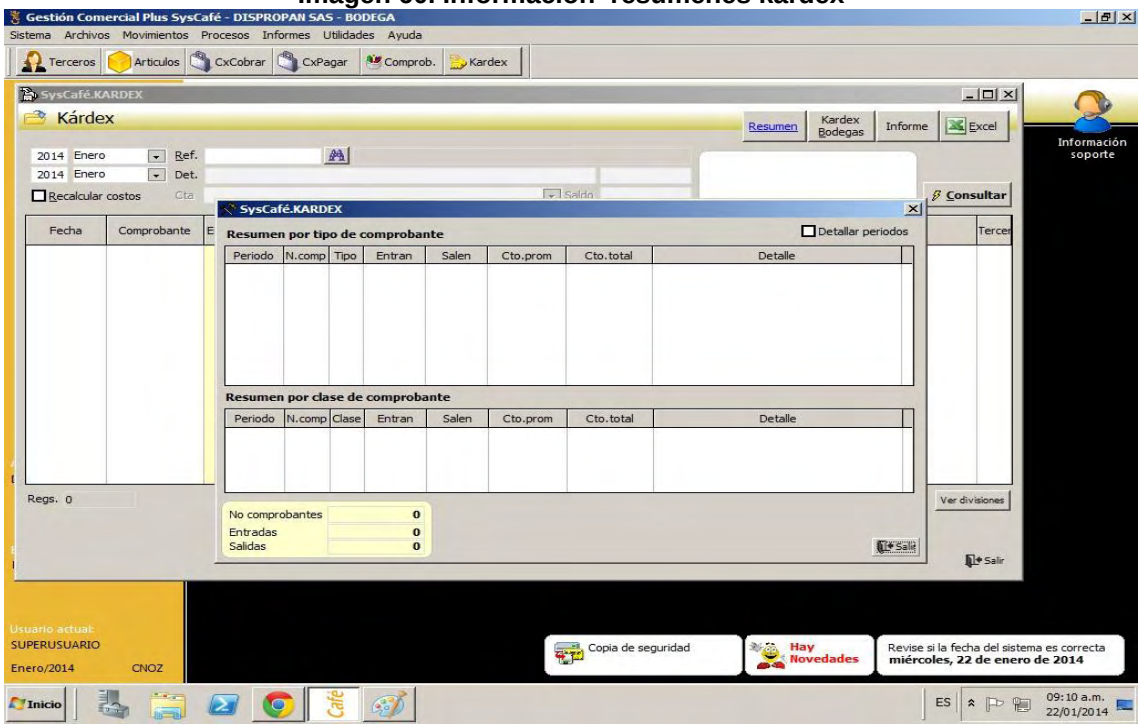


Imagen 61. Información kardex bodega

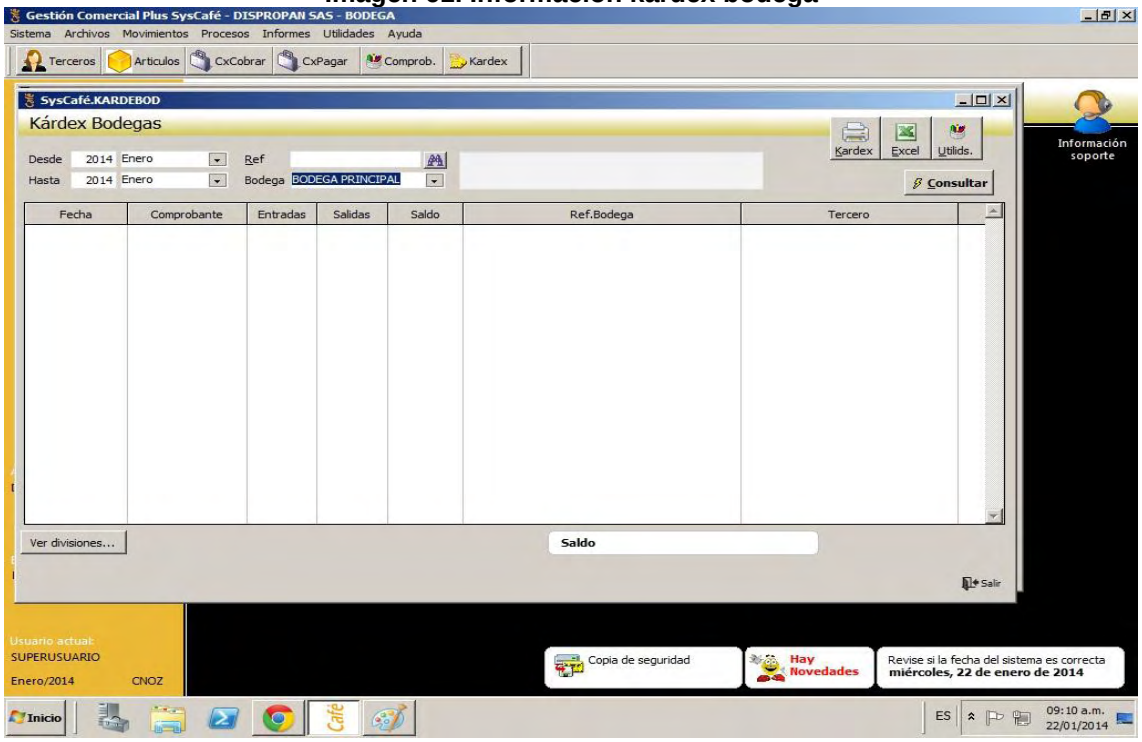


Imagen 62. Información kardex - reportes

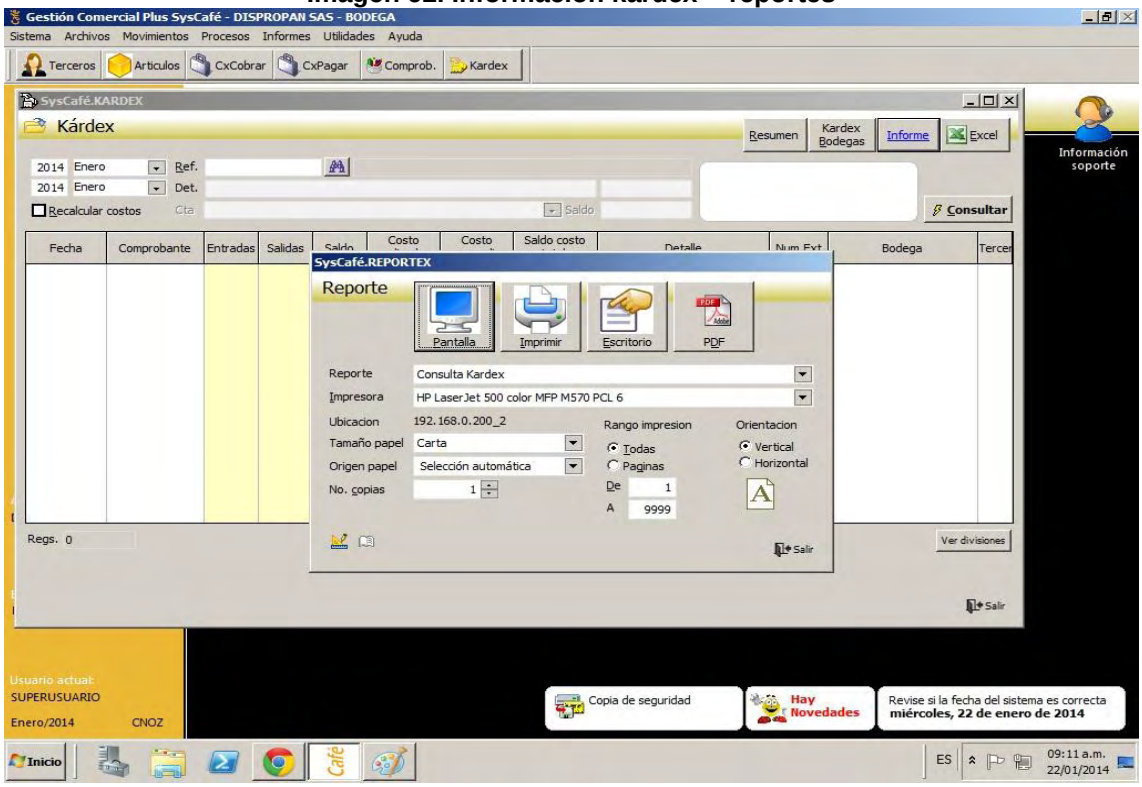


Imagen 63. Ingresos al sistema

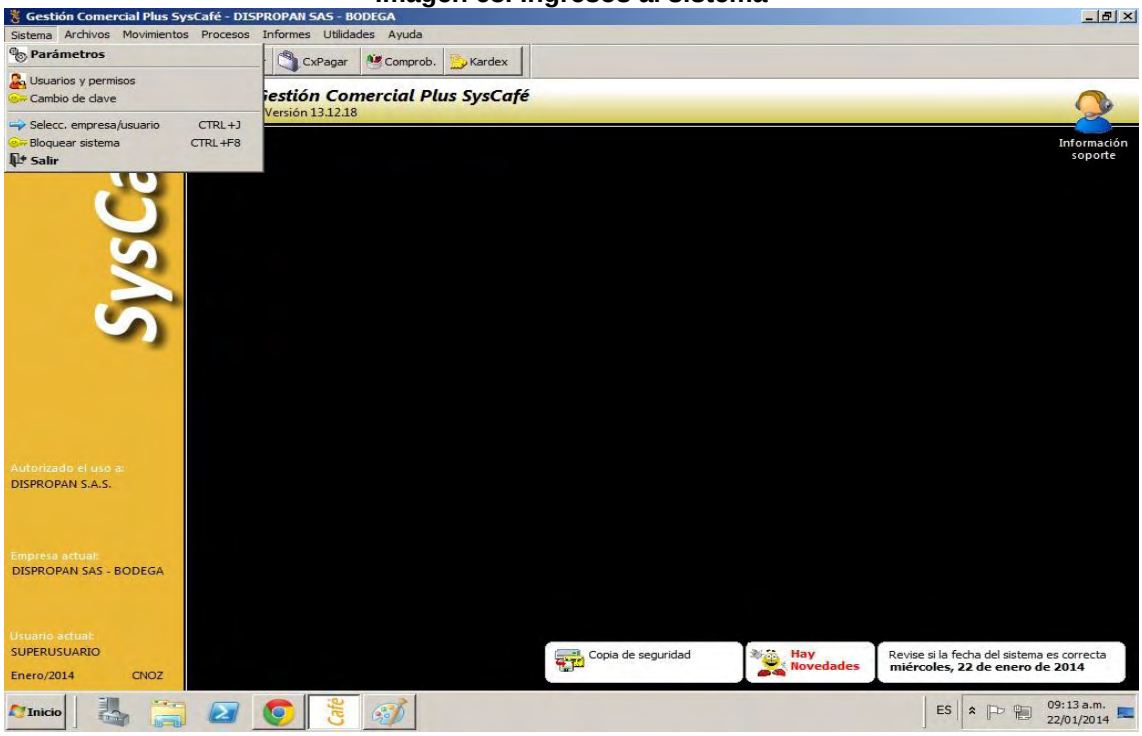


Imagen 64. Ingresos a archivos

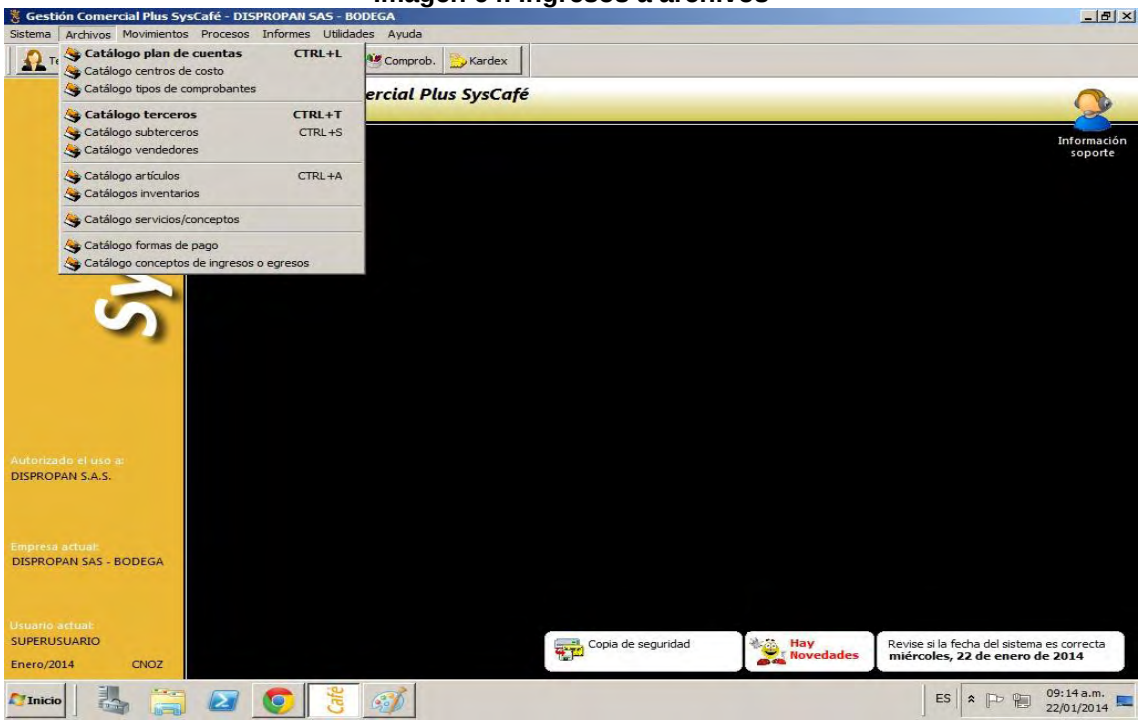


Imagen 65. Ingreso a movimientos del sistema

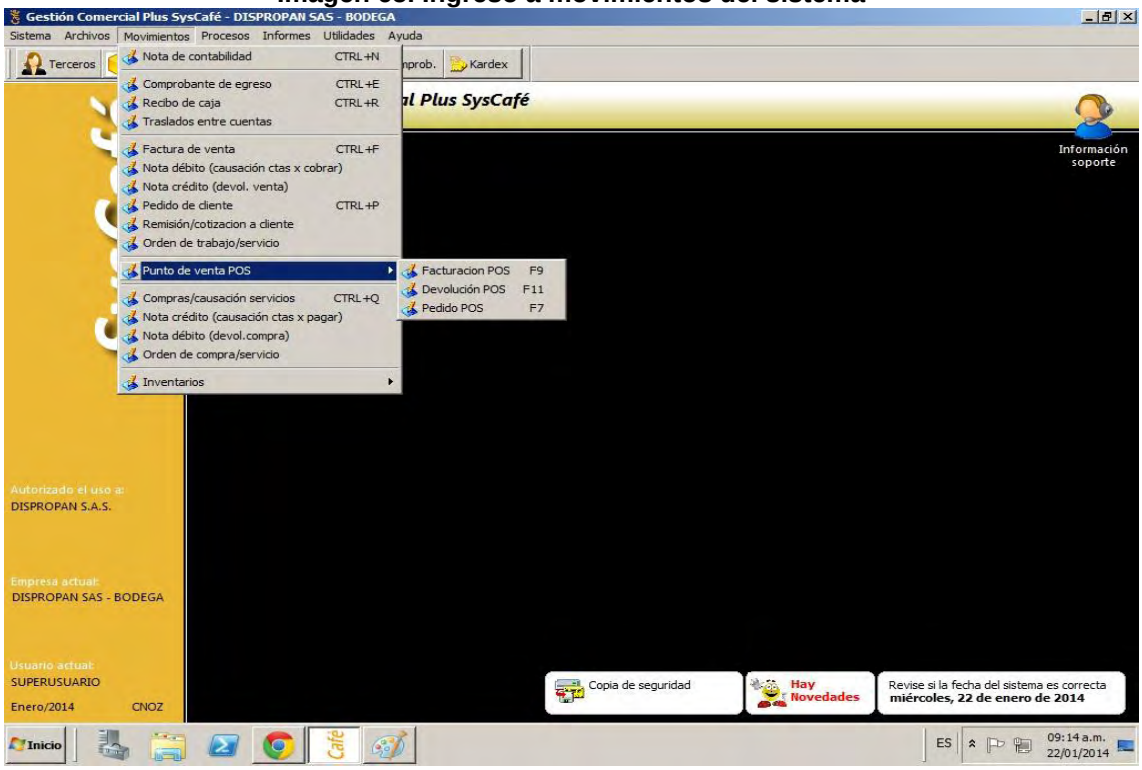


Imagen 66. Ingreso a movimientos tipo inventarios

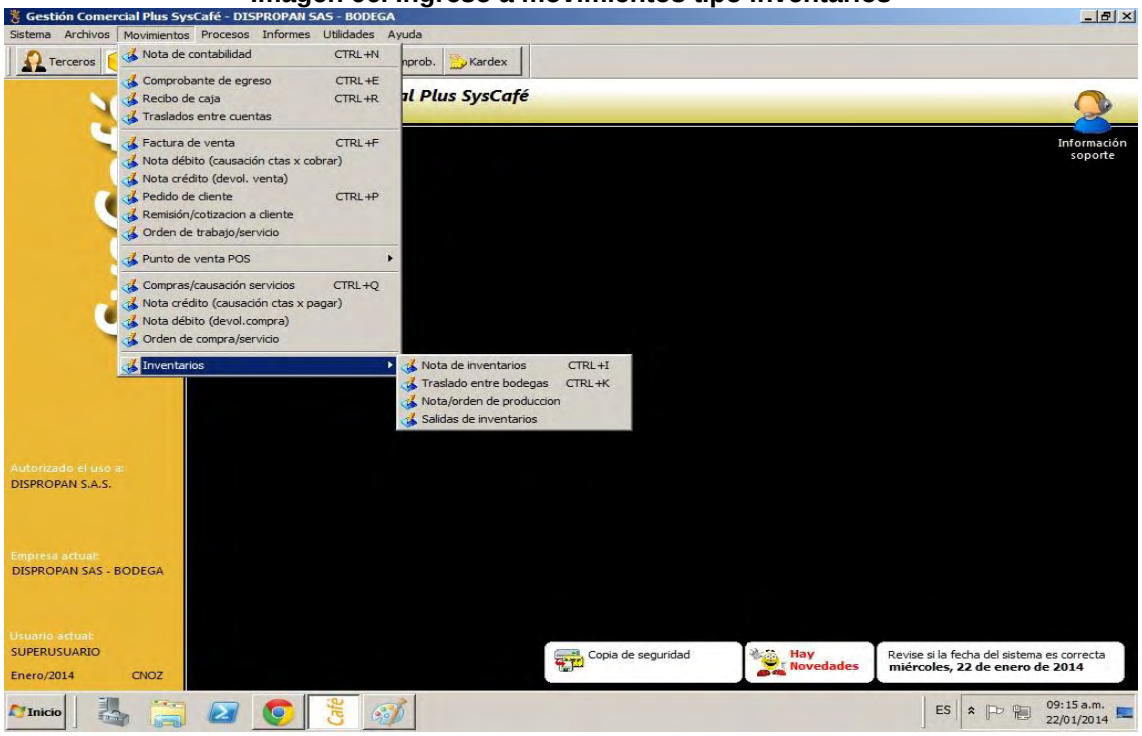


Imagen 67. Ingresar a procesos

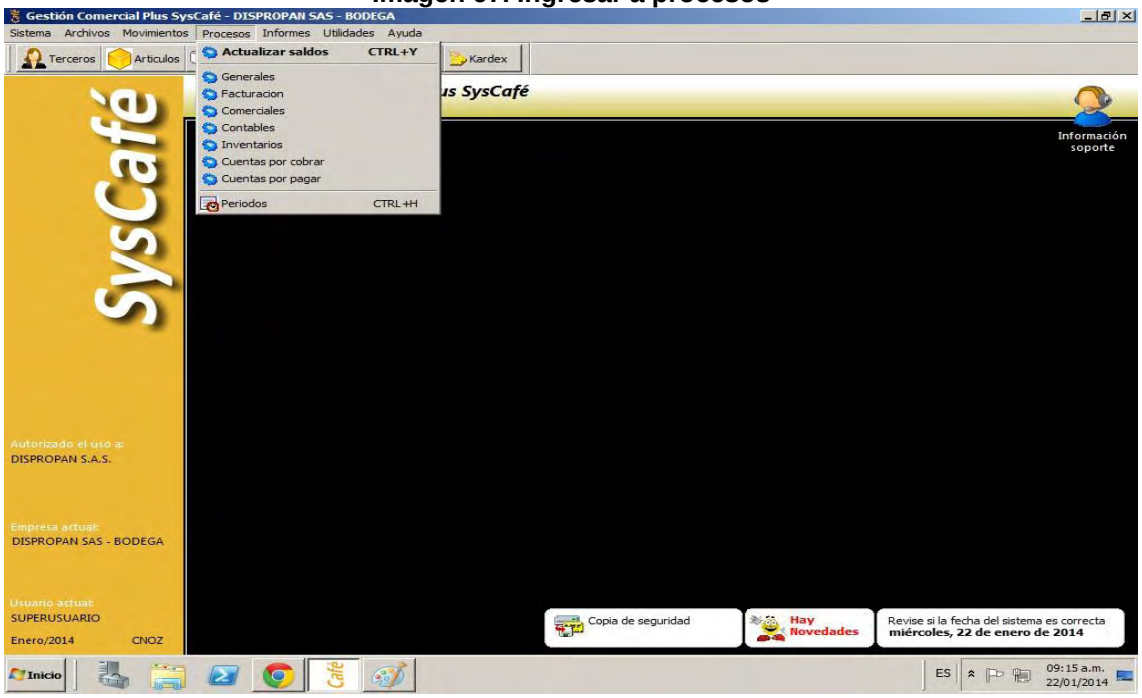


Imagen 68. Ingreso a informes

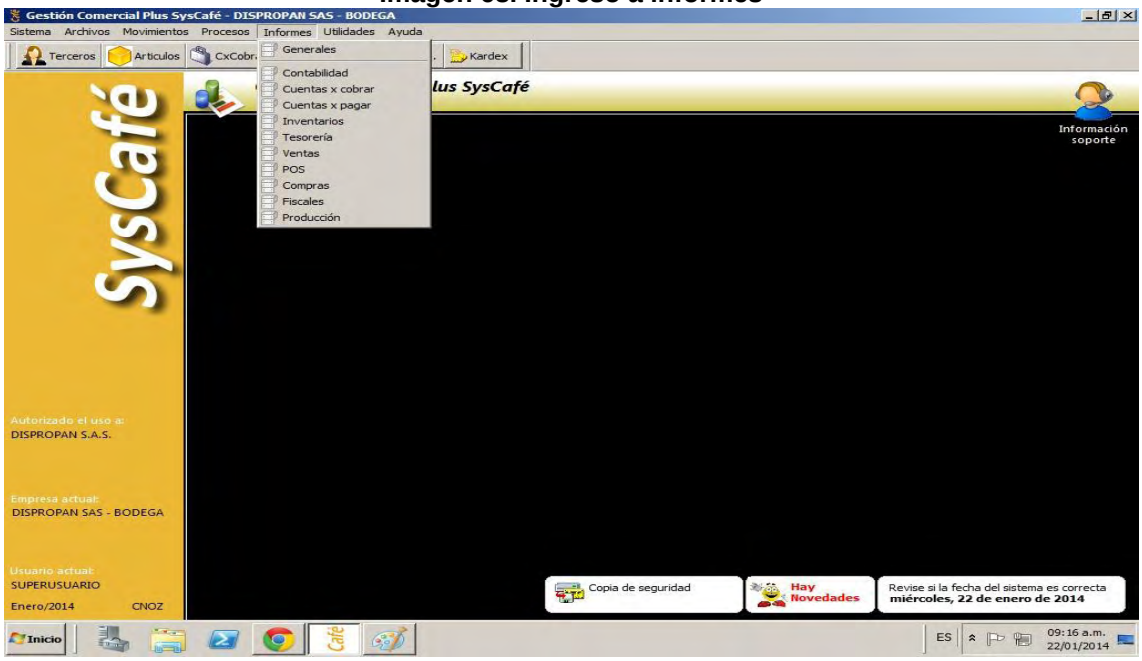


Imagen 69. Ingreso a utilidades

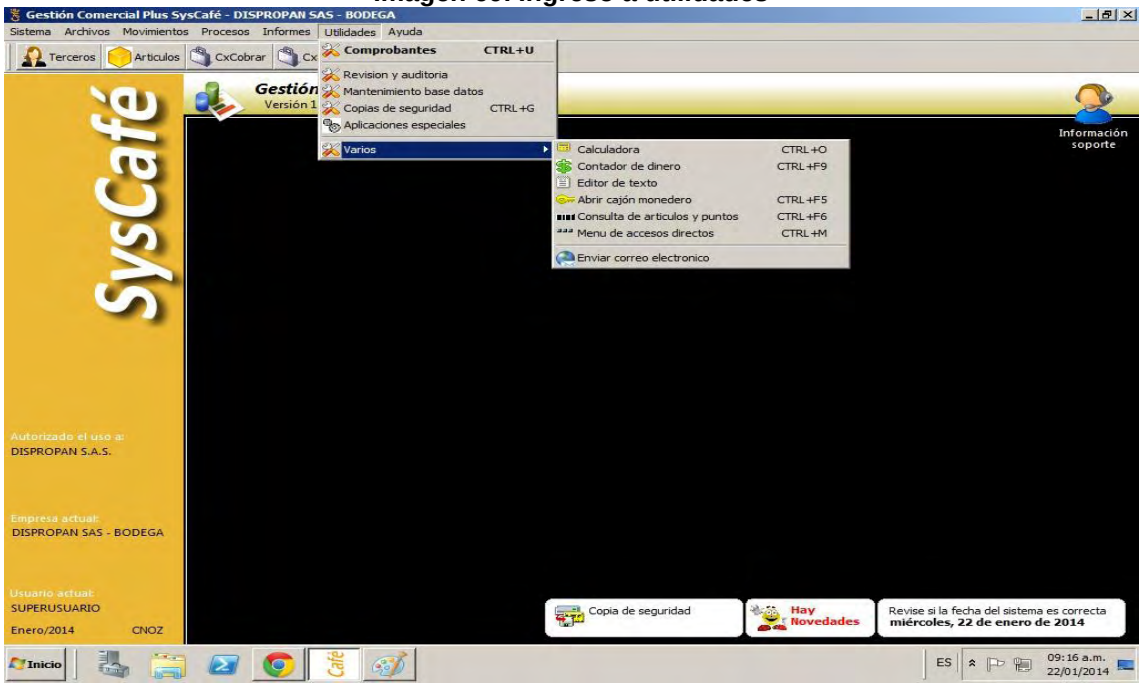
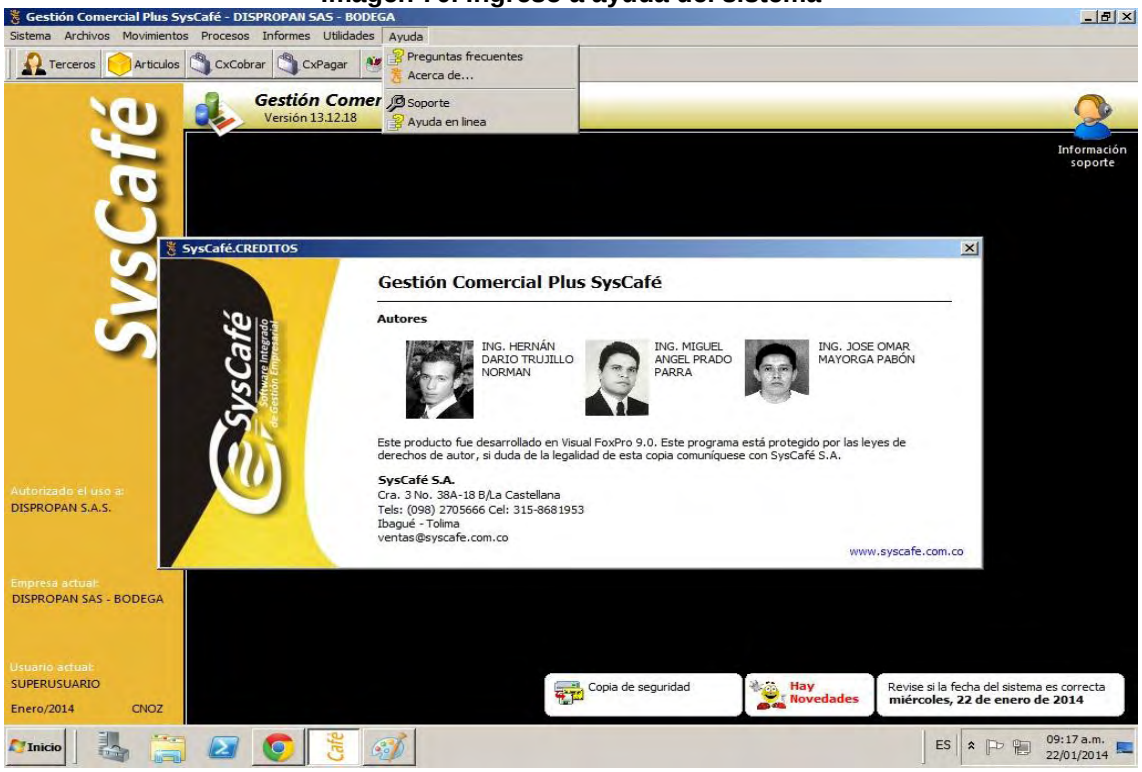


Imagen 70. Ingreso a ayuda del sistema



De igual manera se ven reflejados cada uno de los procesos y los dominios a tener en cuenta en esta auditoría, los encuentra con sus respectivas pruebas, ver anexos carpeta: C: ANEXOS PROCESOS DISPROPAN.

3.2.3 Análisis y evaluación riesgos preliminares

Manual de navegación de hallazgos. En este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

REF: se refiere al ID del elemento.

ENTIDAD AUDITADA: en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: en este espacio se indicara el nombre del proceso objeto de la auditoría.

RESPONSABLES: en este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

HALLAZGO: aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

CONSECUENCIAS Y RIESGOS: en este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

EVIDENCIAS: aquí encontramos en nombre de la evidencia y el número del anexo donde ésta se encuentra.

RECOMENDACIONES: en este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

Dispropan s.a.s.	**HALLAZGO DISPROPAN**	**REF**

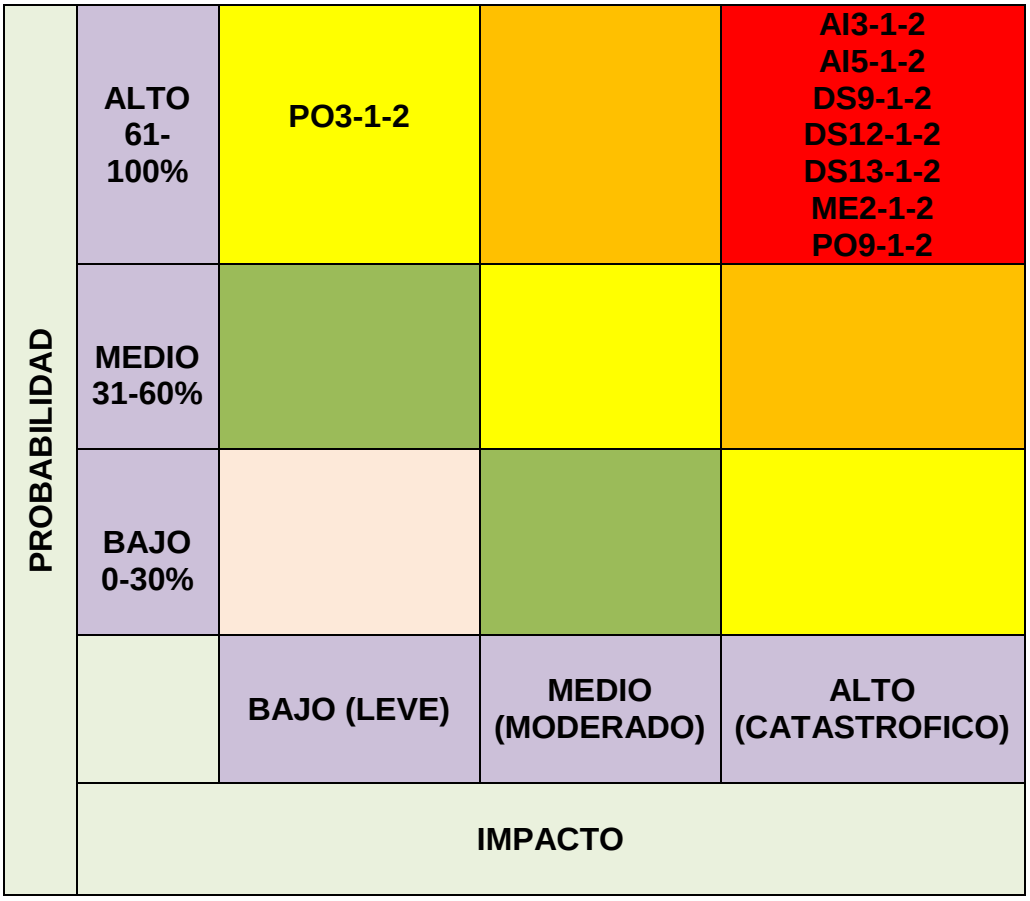
PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**		
		1	DE	1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		
HALLAZGO				

IMPACTO

RECOMENDACIÓN:

PROBABILIDAD – IMPACTO			
Probabilidad		**Impacto**	

Tabla 2. Resultado matriz de probabilidad



3.2.4. Hallazgos. A continuación se describen los hallazgos encontrados en la empresa DISPROPAN SAS.

	HALLAZGO DISPROPAN	REF
		HD_O1

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**		
		1	DE	1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Determinación de dirección tecnológica (PO3)	

HALLAZGO	**En Dispropan SAS,** el plan de contingencia en caso de que el hardware no funcione no está documentado.

RECOMENDACIONES

En la empresa debe existir un documento de plan de contingencia que permita dar solución inmediata en caso de presentarse algún fallo en el hardware.

El documento del plan de contingencia debe contener:

- Objetivos claros para restaurar los servicio de forma rápida, eficiente y en el menor costo y pérdidas posibles.
- Pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional de los servicios.
- Estrategias para la recuperación de desastres.

En cuanto a los diferentes niveles de daños, también se hace necesario presuponer el daño total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

IMPACTO:

El impacto que ocasiona un riesgo de este tipo es la dificultad de recuperación para seguir trabajando en un plazo mínimo después de que se haya presentado un problema, como por ejemplo la posibilidad de volver a la situación anterior, habiendo reemplazado y recuperado el máximo posible de los recursos e información.

En caso de presentarse un fallo del hardware bien sea de un equipo de cómputo o un servidor o un equipo de comunicaciones así haya un proceso practico a seguir este sería solo aplicable por un corto periodo, ya que en caso de un desastre la interrupción prolongada de los servicios de computación y comunicación pueden llevar a pérdidas financieras significativas y pérdida de credibilidad de los usuarios.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Bajo

	HALLAZGO DISPROPAN	**REF**
		HD_O2

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA**	
			1	DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Evaluación De Riesgos(Po9):	
HALLAZGO	En Dispropan SAS no hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de cómputo.			

RECOMENDACIONES

- En Dispropan SAS debe existir un procedimiento que permita realizar el análisis y la gestión de riesgos para el funcionamiento del hardware estos procedimientos deben contener:
  - Objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos.
  - La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los equipos de cómputo.
  - La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones.
  - La determinación del impacto que causaría la ocurrencia de los riesgos.
  - La identificación de controles que mitiguen los riesgos.
  - La toma de decisiones frente a los riesgos.
  - La elaboración del Plan de Seguridad Informática que permita resguardar y mantener los recursos de TI.
  - La ejecución del Plan de Seguridad Informática.
- Es fundamental tener un método para realizar la gestión de riesgos que se integre dentro de la gestión de diferentes proyectos y que así mismo el equipo del proyecto esté involucrado en la identificación y seguimiento de los riesgos.

- Es importante que en la empresa cuente con una herramienta que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del control informático.

IMPACTO

- La gestión de riesgo permite anticiparse al futuro y prevenir a la empresa de diferentes problemas en este caso riesgos que pongan en peligro el buen funcionamiento de la empresa, y el no tener definido políticas de gestión de riesgos implica la toma de decisiones inmediata frente a un problema presentado sin tener previo análisis del riesgo ni tener la certeza de poder mitigar ese riesgo.

- El que no exista personal encargado de la gestión de riesgos del hardware impide la identificación de los posibles riesgos y dado el caso llegase a presentar generaría lo siguiente:

  - Alto costo de la Gestión por Crisis
  - La presencia alta de sorpresas y problemas
  - Perder Ventaja Competitiva
  - Subir variaciones generales del proyecto
  - Disminuir la probabilidad de éxito del proyecto
  - Disminución de rentabilidad
  - Aumentar la probabilidad de la ocurrencia de que se presenten problemas.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF**
		HD_O3

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA**	1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición Y Mantenimiento De La Infraestructura Tecnológica (Ai3):	
HALLAZGO	En Dispropan SAS existe Deficiencia en cuanto al mantenimiento físico de los equipos y actualizaciones de programas de Antivirus.			

RECOMENDACIONES
• Concientización al personal que maneja los equipos de cómputo en cuanto al cuidado y limpieza de estos, puesto que también es responsabilidad de los mismos en el manejo de su herramienta de trabajo. • Actualizar permanentemente el Programa de Antivirus. • El personal de la empresa deberá mantener informado sobre las fechas de mantenimiento, variaciones de los componentes y/o reubicaciones efectuadas a los equipos de cómputo, con el fin de mantener actualizados. • El desarrollo del mantenimiento se efectuara en conformidad con un cronograma establecido, el mismo será coordinado con los funcionarios a fin de tener toda la disponibilidad de los equipos sin afectar sus labores cotidianas. • El mantenimiento preventivo y correctivo es importante hacerlo frecuentemente, muy importante visitar las agencias periódicamente que permita hacer una evaluación del comportamiento de todo lo que tiene que ver con el funcionamiento del hardware y actualizaciones de software que responda a las necesidades del trabajo.

IMPACTO	La falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando en la empresa que los agentes de Contactos permanentemente tengan que estar cambiando de equipos que funcionen entre ellos y más aún cuando un equipo deja de funcionar generara más gastos ya que tendría que cambiarse o reemplazarse algunas piezas del hardware, ya que se disminuye la vida útil de los equipos. La des actualización de vacuna por tener internet genera lentitud y pérdida de información, perjudicando las diferentes tareas de cada agente de contactos.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF**
		HD_O4

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA**	
			1	DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición Y Mantenimiento De La Infraestructura Tecnológica (Ai3):	
HALLAZGO	No hay planos de red de datos de todas las sedes.			

RECOMENDACIONES
• Se recomienda que DISPROPAN SAS, levante planos de red de cableado estructurado, para voz datos, corriente normal y regulada, es muy importante proveerse de planos de todos los pisos de todas las sedes interconectadas, en los que se detallen: - Ubicación de ductos a utilizar para cableado vertical - Disposición detallada de los puestos de trabajo - Ubicación de los tableros eléctricos en caso de ser requeridos • Tener un diagrama de red que permita identificar fácilmente la localización de puntos y equipos en caso de presentarse problemas en la Red. • Así mismo deberá mantener actualizado los planos de red, donde se identifiquen los cambios o expansión de red que se realicen. • El que Dispropan tenga a la mano diseños del cableado estructurado facilitara la administración sencilla y sistemática de los traslados del sitio de trabajo de las personas y equipos. La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, patch panel, armarios de telecomunicaciones y otros espacios ocupados por los sistemas. La norma TIA/EIA 606 proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.

IMPACTO	El no contar con planos de red, en el caso de presentarse fallas en la red, impide que se localice de manera inmediata el punto de fallo, implicando pérdida de tiempo y mayores gastos, teniendo en cuenta que los costos en materiales, mano de obra e interrupción de labores al hacer la búsqueda o hacer cambios en el cableado horizontal pueden ser muy altos. Para la instalación de la red antes se debe realizar el diseño de esta, y se debe tener toda la documentación de los planos, sin embargo el no tenerlos hace que la empresa tenga que contratar personal experto y calificado para el levantamiento de la información y el diseño de la Red, implicando mayores gastos financieros.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF** **HD_O5**

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA** 1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides	
MATERIAL DE SOPORTE	COBIT	

DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición Y Mantenimiento De La Infraestructura Tecnológica (Ai3):

HALLAZGOS	• No existe la implementación del procedimiento de múltiples cotizaciones a diferentes proveedores dentro de las políticas para adquisición de hardware. • No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware. • No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo. • No existe documentación del proceso de mantenimiento de • No existe un centro de cómputo o área de sistemas dentro de la empresa. • No existe proceso de mantenimiento para los elementos como switches, servidores y routers. • No existe un procedimiento específico para el mantenimiento de la red de datos. • No se tiene una implementación adecuada de cableado estructurado. • No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que no existen hojas de vida de los equipos de cómputo. .

IMPACTO:

- Al no existir múltiples cotizaciones para el proceso de adquisición de hardware se puede presentar sobregasto que atenta contra el presupuesto en general de la entidad y el presupuesto destinado a

tecnologías de información.

- Al no existir conocimiento de las políticas de adquisición de hardware por parte de la mayoría de los funcionarios se pierde sentido de pertenencia por la entidad y sus intereses.
- Al no existir documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo se pierde la guía directa de que hacer en este proceso y se presenta retrasó en las actividades.
- Al no existir la elaboración de un acta o documento escrito de la recepción de equipos de cómputo para su respectiva revisión y reparación se carece de información para los objetivos que se plantean en el mantenimiento tanto correctivo o preventivo.
- Al no existir documentación sobre el mantenimiento de los equipos de cómputo se pierde guía de ejecución de este proceso y control de antecedentes.
- Al no existir una persona encargado de hacer mantenimiento de los equipos de cómputo no se optimiza las actividades que deben realizarse en este proceso puesto que no hay responsable concreto para estas funciones.
- Al no existir la conformación del centro de cómputo se atenta contra la normatividad que busca en muchos aspectos brindar seguridad para la información y optimización de procesos.
- Al no existir el proceso de mantenimiento para los elementos como swiches, routers y servidores se atenta contra el buen funcionamiento de estos elementos y contra el cuidado que se les debe brindar ya son pieza fundamental de la red de datos.
- Al no existir un proceso de mantenimiento especifico de la red de datos se atenta contra su óptimo funcionamiento y prevención de sucesos que perjudiquen los procesos que relacionan al sistema de red de datos.
- Al no hacer seguimiento adecuado de los elementos como son routers, switches y servidores mediante hojas de vida ajustadas a recolectar la información suficiente se pierden los antecedentes que a futuro se deben utilizar para prevención y corrección de eventos que afecten el funcionamiento de estos elementos o equipos.

RECOMENDACIONES:

- Implementar dentro del proceso de adquisición de hardware el requisito de múltiples cotizaciones para con ello proteger el presupuesto de la entidad destinado a tecnologías de información.
- Dar a conocer las políticas de adquisición de hardware a los funcionarios para tener mayor sentido de pertenencia por los intereses de la entidad.
- Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.

- Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.
- Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.
- Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.
- Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la empresa.
- Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.
- Elaborar hojas de vida adecuadas para recolectar información que sirva para el óptimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF**
		HD_O6

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**	1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds5)

HALLAZGO	• El personal de la empresa no cuenta con una debida capacitaciones sobre el manejo del software GESTION SYSCAFE • No se tiene un control de cuentas de usuarios • No se tiene documentación de los permisos a usuarios del software GESTION SYSCAFE • No se cuenta con documentación de la seguridad de hardware y software de la empresa. • No se tiene procesos de Prevención, detección y corrección de software malicioso que garantice medidas de prevención, detección y corrección para proteger a los sistemas de información

IMPACTO:

- Al no tener una capacitación total del software GESTION SYSCAFE se corre el riesgo de un mal manejo de la información.
- El software de GESTION SYSCAFE permite la creación de varios usuarios con diferentes permisos para lo cual el mal manejo de esto hace que el personal pueda tener acceso a enlaces no necesarios e importantes para el manejo de información de la empresa.
- Al no contar con un documento de los permisos dados al personal que maneja el software GESTION SYSCAFE no se puede tener un control del manejo y manipulación de la información que tiene el personal.
- Al no tener procesos de prevención y detección de software malicioso no se puede controlar la seguridad de la información que se maneja en la empresa DISPROPAN SAS.

RECOMENDACIONES:

- Es necesario se de las capacitaciones oportunas al personal que maneja el

software GESTION SYSCAFE para que puedan ingresar la información de manera correcta evitando así futuras pérdidas de tiempo e información en correcciones. • Es necesario la documentación de los permisos que da el software de GESTION SYSCAFE para mantener un continuo control del manejo de la información y el acceso a ella. • Teniendo en cuenta que la información que maneja el personal de DISPROPAN es diferente teniendo en cuenta el cargo y sus funciones frente a esta información es necesario llevar un control del manejo de los permisos que tienen para la manipulación de la información por medio de las cuentas de usuarios que tiene el software. • Es necesario buscar procesos de prevención y detección de software malicioso para de esa manera controlar la seguridad de la información que se maneja en la empresa DISPROPAN SAS.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF**
		HD_O7

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software	**PÁGINA**	1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds12)

HALLAZGO	• El espacio donde se encuentra ubicado los equipos de internet (Modem) rack, Switch y cableado de datos no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura).

RECOMENDACIONES
En la empresa DISPROPAN SAS es necesario tener en cuenta que el espacio donde está ubicado el internet (Modem) rack, Switch y cableado de datos debe cumplir con la norma ANSI/TIA/EIA-569-A a fin de mejorar la seguridad. Los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

IMPACTO:
Los equipos activos (switches, router, etc) así como los cables quedan expuestos completamente al polvo y humedad, provocando daños y/o pérdidas de equipos.

Los equipos activos están expuestos a caídas, por estar en el mismo espacio de las oficinas de atención al cliente, las conexiones en los equipos o en el panel de empalme pueden ser manipuladas por cualquier persona.

El daño o pérdida de algún equipo activo genera pérdida de información o el cambio de equipos por consiguiente gastos para comprar o remplazar equipos.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	REF
		HD_O7_1

REF:	OFICINA PRINCIPAL_DISPROPAN

REF:	OFICINA PRINCIPAL_DISPROPAN

	HALLAZGO DISPROPAN	**REF**
		HD_O8

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA**	1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds12)	

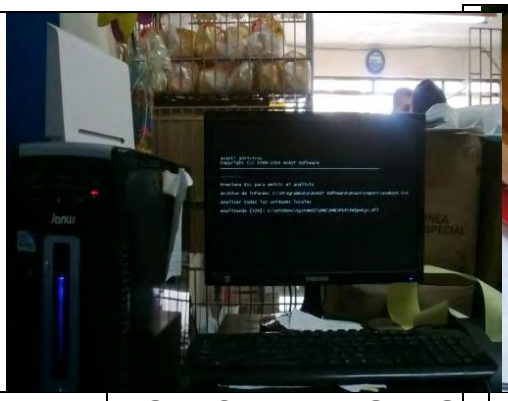
HALLAZGO	• En la Agencia Ipiales el espacio donde se encuentra ubicado el equipo de cómputo, equipo de internet (Modem) y cableado de datos no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura).

RECOMENDACIONES
En la Agencia Ipiales es necesario tener en cuenta que el espacio donde está ubicado el internet (Modem) rack, Switch y cableado de datos debe cumplir con la norma ANSI/TIA/EIA-569-A a fin de mejorar la seguridad. Los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

IMPACTO:
Los equipos activos están expuestos a caídas, por estar en el mismo espacio de las oficinas, las conexiones en los equipos o en el panel de empalme pueden ser manipuladas por cualquier persona. El daño o pérdida de algún equipo activo genera pérdida de información o el cambio de equipos por consiguiente gastos para comprar o remplazar equipos.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	**REF**
		HD_O8_1



REF:	AGENCIAIPIALES_DISPROPAN

REF:	AGENCIAIPIALES_DISPROPAN

REF:	AGENCIAIPIALES_ DISPROPAN

	HALLAZGO DISPROPAN	**REF**
		HD_O9

PROCESO AUDITADO	Indicadores de funcionamiento del hardware y software		**PÁGINA**	1 DE 1
RESPONSABLE	Jhoana Lorena Hernández Benavides			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicio y Soporte (Ds)	**PROCESO**	Garantizar La Seguridad De Sistemas (Ds12)	

HALLAZGO	• En la Agencia Pasto el espacio donde se encuentra ubicado el equipo de cómputo, equipo de internet (Modem) y cableado de datos no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura).

RECOMENDACIONES
En la Agencia Pasto es necesario tener en cuenta que el espacio donde está ubicado el internet (Modem) rack, Switch y cableado de datos debe cumplir con la norma ANSI/TIA/EIA-569-A a fin de mejorar la seguridad. Los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

IMPACTO:
Los equipos activos están expuestos a caídas, por estar en el mismo espacio de las oficinas, las conexiones en los equipos o en el panel de empalme pueden ser manipuladas por cualquier persona. El daño o pérdida de algún equipo activo genera pérdida de información o el cambio de equipos por consiguiente gastos para comprar o remplazar equipos.

PROBABILIDAD – IMPACTO			
Probabilidad	Alto	**Impacto**	Alto

	HALLAZGO DISPROPAN	REF
		HD_O8_1

REF:	AGENCIA_PASTO_DISPROPAN

REF:	AGENCIA_PASTO_DISPROPAN

3.2.4. Informe de Auditoría:

- ✓ **Objetivos**

Evaluar la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, los servidores y el funcionamiento del sistema SYSCAFE para en la empresa DISPROPAN S.A.S, con el propósito de ayudar a definir y establecer un plan de mejoramiento e integración de tecnología.

- ✓ **Objetivos específicos**

Identificar los posibles puntos críticos dentro de los procesos del hardware, en cuanto a servidores, equipos de cómputo e indicadores de funcionamiento real de la empresa.

Identificar falencias en la parte de hardware de equipos de cómputo, en cuanto al sistema de información SYSCAFE, contratos y soporte, mediante las prácticas de auditoría.

Garantizar el correcto funcionamiento del Hardware de cómputo, procesos e información de la empresa DISPROPAN S.A.S

- ✓ **Limitaciones**

La auditoría se realizó con completa normalidad, cabe resaltar la colaboración de todo el personal de la empresa DISPROPAN SAS para hacer posible la toma de datos y la realización de todos los procesos aplicados en el COBIT.

- ✓ **Resultados de la Auditoría**

A continuación se presentan los resultados de la auditoría aplicada a la empresa DIPROPAN SAS, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditados.

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

Proceso COBIT PO3: Determinación de dirección tecnológica:

Hallazgo: en Dispropan SAS, el plan de contingencia en caso de que el hardware no funcione no está documentado.

Recomendaciones: en la empresa debe existir un documento de plan de contingencia que permita dar solución inmediata en caso de presentarse algún fallo en el hardware.

El documento del plan de contingencia debe contener:

- Objetivos claros para restaurar los servicio de forma rápida, eficiente y en el menor costo y pérdidas posibles.
- Pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional de los servicios.
- Estrategias para la recuperación de desastres.
- En cuanto a los diferentes niveles de daños, también se hace necesario presuponer el daño total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

REF: HD_01

Proceso COBIT PO9: evaluación de riesgos

Hallazgo: en Dispropan SAS no hay política o procedimientos para el análisis y gestión de riesgo para el funcionamiento del hardware de los equipos de cómputo.

Recomendaciones: en Dispropan SAS debe existir un procedimiento que permita realizar el análisis y la gestión de riesgos para el funcionamiento del hardware estos procedimientos deben contener:

- Objetivos que se pretende alcanzar con la aplicación de la gestión de los riegos.
- La identificación y clasificación de los riesgos a los que se encuentra expuesto el hardware de los equipos de cómputo.
- La determinación de la probabilidad de ocurrencia de los riesgos que amenazan el funcionamiento del hardware de los equipos de cómputo, los servidores y las comunicaciones.
- La determinación del impacto que causaría la ocurrencia de los riesgos.
- La identificación de controles que mitiguen los riesgos.
- La toma de decisiones frente a los riesgos.
- La elaboración del plan de seguridad informática que permita resguardar y mantener los recursos de TI.
- La ejecución del plan de seguridad informática.

- Es importante que en la empresa cuente con una herramienta que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del control informático.
- Es fundamental tener un método para realizar la gestión de riesgos que se integre dentro de la gestión de diferentes proyectos y que así mismo el equipo del proyecto esté involucrado en la identificación y seguimiento de los riesgos.

REF: HD_02

DOMINIO: ADQUISICION E IMPLEMENTACION (AI)

Proceso COBIT AI3: adquisición Y mantenimiento de la infraestructura Tecnológica:

Hallazgo: en Dispropan SAS existe Deficiencia en cuanto al mantenimiento físico de los equipos y actualizaciones de programas de Antivirus.

No hay planos de red de todas de todas las Agencias.

No existe la implementación del procedimiento de múltiples cotizaciones a diferentes proveedores dentro de las políticas para adquisición de hardware.

No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.

No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo.

No existe documentación del proceso de mantenimiento

No existe un centro de cómputo o área de sistemas dentro de la empresa.

No existe proceso de mantenimiento para los elementos como switches, servidores y routers.

No existe un procedimiento específico para el mantenimiento de la red de datos.

No se tiene una implementación adecuada de cableado estructurado.

No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que no existen hojas de vida de los equipos de cómputo.

Recomendaciones: concientizar al personal que maneja los equipos de cómputo en cuanto al cuidado y limpieza de estos, puesto que también es responsabilidad de los mismos en el manejo de su herramienta de trabajo.

- Actualizar permanentemente el Programa de Antivirus.
- El personal de la empresa debe mantener informado sobre las fechas de mantenimiento, variaciones de los componentes y/o reubicaciones efectuadas a los equipos de cómputo, con el fin de mantener actualizados.

- El mantenimiento preventivo y correctivo es importante hacerlo frecuentemente, muy importante visitar las agencias periódicamente que permita hacer una evaluación del comportamiento de todo lo que tiene que ver con el funcionamiento del hardware y actualizaciones de software que responda a las necesidades del trabajo.
- El desarrollo del mantenimiento se efectuara en conformidad con un cronograma establecido, el mismo será coordinado con los funcionarios a fin de tener toda la disponibilidad de los equipos sin afectar sus labores cotidianas
- Se recomienda que DISPROPAN SAS, levante planos de red de cableado estructurado, para voz datos, corriente normal y regulada, es muy importante proveerse de planos de todos los pisos de todas las sedes interconectadas, en los que se detallen:
    - Ubicación de ductos a utilizar para cableado vertical
    - Disposición detallada de los puestos de trabajo
    - Ubicación de los tableros eléctricos en caso de ser requeridos
    - Tener un diagrama de red que permita identificar fácilmente la localización de puntos y equipos en caso de presentarse problemas en la Red.
- Así mismo deberá mantener actualizado los planos de red, donde se identifiquen los cambios o expansión de red que se realicen.
- El que Dispropan tenga a la mano diseños del cableado estructurado facilitara la administración sencilla y sistemática de los traslados del sitio de trabajo de las personas y equipos. La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, patch panel, armarios de telecomunicaciones y otros espacios ocupados por los sistemas. La norma TIA/EIA 606 proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.
- Implementar dentro del proceso de adquisición de hardware el requisito de múltiples cotizaciones para con ello proteger el presupuesto de la entidad destinado a tecnologías de información.
- Dar a conocer las políticas de adquisición de hardware a los funcionarios para tener mayor sentido de pertenencia por los intereses de la entidad.
- Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.
- Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.
- Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.
- Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.

- Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la empresa.
- Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.
- Elaborar hojas de vida adecuadas para recolectar información que sirva para el óptimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro

REF: HD_03, HD_04, HD_05,

Dominio: entrega de servicio y soporte

Proceso Cobit DS5: garantizar la seguridad de sistemas

Hallazgos:

- El personal de la empresa no cuenta con una debida capacitaciones sobre el manejo del software GESTION SYSCAFE

- No se tiene un control de cuentas de usuarios

- No se tiene documentación de los permisos a usuarios del software GESTION SYSCAFE

- No se cuenta con documentación de la seguridad de hardware y software de la empresa.

- No se tiene procesos de Prevención, detección y corrección de software malicioso que garantice medidas de prevención, detección y corrección para proteger a los sistemas de información

Recomendaciones:

- Es necesario se de las capacitaciones oportunas al personal que maneja el software GESTION SYSCAFE para que puedan ingresar la información de manera correcta evitando así futuras pérdidas de tiempo e información en correcciones.
- Es necesario la documentación de los permisos que da el software de GESTION SYSCAFE para mantener un continuo control del manejo de la información y el acceso a ella.
- Teniendo en cuenta que la información que maneja el personal de DISPROPAN es diferente teniendo en cuenta el cargo y sus funciones frente a

esta información es necesario llevar un control del manejo de los permisos que tienen para la manipulación de la información por medio de las cuentas de usuarios que tiene el software.

- Es necesario buscar procesos de prevención y detección de software malicioso para de esa manera controlar la seguridad de la información que se maneja en la empresa DISPROPAN SAS

REF: HD_06

✓ **Proceso Cobit DS12: garantizar la seguridad de sistemas:**

Hallazgos: el espacio donde se encuentra ubicado los equipos de internet (Modem) rack, Switch y cableado de datos no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura).

En la agencia Ipiales el espacio donde se encuentra ubicado el equipo de cómputo, equipo de internet (Modem) y cableado de datos no se acoge a la norma EIA/TIA 569A. (Movilidad, altura, anchura).

Recomendaciones:

- En la empresa DISPROPAN SAS es necesario tener en cuenta que el espacio donde está ubicado el internet (Modem) rack, Switch y cableado de datos debe cumplir con la norma ANSI/TIA/EIA-569-A a fin de mejorar la seguridad.
- Los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete

REF: HD_07, HD_7_1, HD_8, HD_8_1.

Informe gerencial de auditoría:

San Juan de Pasto

Sr:
FRANCISCO GUTIERREZ
Gerente DISPROPAN SAS
Ciudad

REF: AUDITORÍA INFORMÁTICA A NIVEL DE LOS SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO.

Cordial Saludo,

El presente es el informe de la auditoría a la que fue sometida su empresa, con el objetivo de evaluar los procesos de los sistemas e indicadores de funcionamiento del hardware y el software.

Los resultados obtenidos son producto de la aplicación de técnicas y herramientas de auditoría, teniendo como base la información y documentación que fue suministrada por el personal laboral de la empresa.
Los resultados obtenidos se sustentan como hallazgos con sus respectivas recomendaciones y en algunos casos fortalezas encontradas. Estas son:

Teniendo en cuenta que uno de los procesos principales que mueve a la empresa DISPROPAN SAS es las ventas se tiene en cuenta lo siguiente:

PROCESO DE VENTAS: En cuanto a la atención al cliente de los punto de venta es importante que los vendedores tengan en cuenta que aparte de productos venden una imagen , una marca, venden calidad y por lo tanto también es importante que lo hagan con calidez para ello se sugiere una capacitación de ATENCION AL USUARIO, ya que como ejemplo real puedo citar que “se presentó la Sra. Cruz Ana Guerrero a comprar unos productos y luego de esto le manifestó a Jhoana Hernández que estaba insatisfecha con la atención brindada pues no le brindaron la información que necesitaba y el genio de quien le vendió fue terrible y de afán”; para lo anterior se sugiere adicional a la capacitación el colocar un buzón de sugerencias por agencia o punto de venta ya que una queja es una oportunidad para mejorar y conocer la opinión del cliente sobre el servicio ya que una queja sirve para :

- **conocer** la percepción que el cliente tiene de nuestros servicios.
- **sirve de guía** para mejorar, pues se puede corregir defectos o errores que repetimos sistemáticamente sin darnos cuenta.

- **Son una oportunidad** para afianzar la relación con el cliente, se sentirá atendido, escuchado, y como parte valiosa que aporta información de mejora a la empresa.
- **facilitan información** acerca de las necesidades y expectativas de los clientes.

Porque puede haber clientes insatisfechos que no se quejan, y solo se conoce su malestar cuando se van y es precisamente esto lo que se quiere evitar.

Plan de contingencia: en caso de que el hardware no funcione no existe un plan de contingencia documentado.

El no contar con un plan de contingencia dificulta la recuperación de seguir trabajando en un plazo mínimo después de que se haya presentado un problema o desastre inesperado, en caso de presentarse un fallo del hardware la solución de un proceso practico a seguir sería aplicable para un problema técnico y pequeño pero no para un desastre o catástrofe, la interrupción de los servicios de computación y comunicación seria prolongada llevando a las empresas pérdidas financieras significativas.

En la empresa debe existir un plan de contingencia documentado que permita dar solución inmediata, este debe contener objetivos de cómo restaurar los servicios de forma rápida, eficiente y con el menor tiempo, costos y pérdidas posibles.

La empresa actualmente cuenta con personal capaz de solucionar cualquier problema que se presente aun cuando el plan de contingencia no esté documentado aunque cuando esta presentes terceros estos problemas toman su tiempo haciendo que se vean reflejados los resultados en pérdidas.

Ejemplo claro es el presentado el 16 de mayo que por solicitud de un proceso con el proveedor de internet nos quedamos sin sistema desde el 16 al 19 de mayo haciendo que el sistema informático no funcione en la empresa y que provoque perdidas en la empresa ya que se tiene que acudir al sistema antiguo del manejo del papel, lo resaltable en esta situación es el trabajo en equipo por el personal de la empresa que logró minimizar el tiempo de espera para la solución del problema.

Evaluación del hardware de equipos de cómputo, dispositivos móviles y redes:

- **la existencia de inventarios:** la empresa DISPROPAN SAS no tiene un manejo adecuado de un inventario tecnológico, por lo cual es importante sugerir la creación de este inventario y mantenerlo actualizado constantemente para llevar un control y/o registro adecuado de los activos de la empresa.

- **los procesos de mantenimiento:** es muy importante llevar un proceso documentado de los procesos de mantenimiento tanto de hardware como de software en la sede principal y en las agencias esto con el fin de llevar un control de la vida útil de cada uno de los elementos tecnológicos de la empresa para futuras tomas de decisiones y mejoramientos de la empresa. la falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando perdida de información o peor aun cuando un equipo deja de funcionar generara más gastos.

  se recomienda periódicamente visitar las sedes o establecer medidas que permitan hacer una evaluación continua de las necesidades que se presenten en ellas, con el fin de solventar fallas en los diferentes procesos o actividades de los usuarios, así mismo cuando se reciba reportes de fallas de parte de las agencias estableces un periodo de tiempo mínimo para dar solución, esto con el fin de no alargar mucho tiempo en resolver el problema ya sea de hardware o software.también es necesario concientizar al personal que maneja los equipos de cómputo en cuanto al cuidado y limpieza, dar a conocer con anterioridad el cronograma de mantenimiento al personal porque muchas veces las actividades se ven interrumpidas debido al mantenimiento.

- **la actualización de equipos:** la empresa Dispropan maneja equipos tecnológicos que van a la par con el avance tecnológico pero no manejan un sistema de actualización para los equipos existentes ni tampoco una documentación de los mismos, para lo cual se recomienda programar las actualizaciones de software que responda a las necesidades del trabajo a realizar en cada una de las sedes dependiendo de los equipos y las actualizaciones necesarias para no entorpecer las actividades diarias.

- **actualización de dispositivos de red:** Se recomienda mantener actualizados los planos de la red de voz y datos, donde se puede evidenciar los elementos de la red como gabinetes de comunicaciones, puestos de trabajo, puntos de red, cuellos de botella, entre otros, esto con el fin de identificar problemas y sorpresas que se pueden presentar y cambios que se pueden realizar.

- **adquisición de equipos:** no se encontró una documentación sobre cómo se lleva a cabo los procesos de adquisición de infraestructura tecnológica pero cabe resaltar que el personal está pendiente de cada una de las necesidades en cuanto a equipos necesarios y se tiene en cuenta la mejor opción a la hora de adquirir los equipos tecnológicos.

- **configuración e instalación de redes:** en DISPROPAN SAS no existe documentación de la gestión de red de comunicaciones, en caso de presentarse fallas, el no contar con planos de red, impide que se localice de

manera inmediata el punto de fallo implicando pérdida de tiempo y mayores gastos, teniendo en cuenta que los costos en materiales, mano de obra e interrupción de labores al hacer la búsqueda o hacer cambios en la infraestructura pueden ser muy altos.

Aunque no haya planos de red, mediante la aplicación de técnicas de auditoría se identifica que DISPROPAN SAS cuenta con una red de datos aceptable, pues tanto su distribución como los equipos son adecuados a las funciones del puesto de trabajo.
Se recomienda que se cuente con un documento de gestión de red, el cual permita identificar objetivos encaminados a la monitorización del tráfico y la calidad del servicio, pautas que permitan prevenir, diagnosticar y resolver problemas de la red. Identificación de los usuarios de la red y el software, dar soporte a los usuarios, pautas de seguridad, gestión de los fallos producidos en la red, gestión de rendimiento y planificación.

Se recomienda además que los equipos activos (switche, router, etc) se acojan a la norma ANSI/TIA/EIA-569-A, los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

Evaluación de área informática y funciones del personal de informática:

- actualmente no se encuentra creada como tal el área de informática en DISPROPAN SAS por lo que se recomienda consolidarla con una persona encargada de esta área y de la creación y mantenimiento de todos los procesos necesarios a llevar, la persona encargada de esta área se recomienda sea una persona idónea en este campo que sepa el manejo de la infraestructura tecnológica y el manejo de los procesos para la misma, además de tener conocimientos en sistemas y procesos informáticos, ya que actualmente cuando se presentan problemas informáticos y tecnológicos el personal de la empresa debe de alguna manera buscar la solución con personal diferentes a los existentes en la empresa.

Evaluación del sistema de información SYSCAFE:

- **Funcionalidad del sistema:** la empresa DISPROPAN SAS trabaja con la empresa SYSCAFE el cual les brinda el producto de GESTION el cual cuenta con módulos de Contabilidad, Facturación Y Ventas, Tesorería, Cuentas Por Cobrar Y Pagar, Inventarios. El software es manejado por el personal de la empresa teniendo cada usuario permisos específicos para la manipulación de datos, el software funciona bien, teniendo en cuenta que se presentan errores e inconvenientes por mala manipulación de los usuarios así como también se presentan errores porque el sistema está constantemente actualizándose y por

lo cual se observan errores en informes como cierres de cajas, descuentos, mal llamado a las cuentas para los informes de carteras, entre otros. A lo anterior se sugiere llevar un control del soporte realizado por SYSCAFE ya que no todos los soportes son por causa de mala manipulación de la información por parte del personal de DISPROPAN, sino por errores presentados en los informes que arroja el software y por fallas en validaciones de la información, para ejemplo de esta validación tenemos el campo de móvil o teléfono en la creación de terceros en la cual me admite cualquier carácter y cualquier longitud y por lo cual genera errores posteriores para la generar informes, especialmente los que se realizan para la DIAN y SYSCAFE tiene claridad de estos datos.

Ante lo anterior también se debe tener en cuenta lo presentado en la segunda semana de mayo ante un inconveniente con la actualización del software gestión de SYSCAFE por lo cual se eliminaron los usuarios existentes en el sistema y fue necesario crear nuevamente los usuarios que ingresan al sistema y dar el correspondiente permiso a los paquetes o informes del mismo, esto no ocasionó perdida de información.

Para lo anterior se sugiere:

- Que el usuario SUPERUSUARIO lo maneje una sola persona, permitiendo así tener el control de los permisos otorgados a los usuarios del sistema.
- El usuario SUPERUSUARIO sea utilizado única y exclusivamente para modificaciones del software, cambio de parámetros de la empresa y la administración de los usuarios y sus permisos.
- Cada usuario es responsable de los movimientos que haga con el mismo.

Las entradas del sistema: teniendo en cuenta los diferentes permisos que los usuarios tienen para la manipulación del software gestión de SYSCAFE a diario se está entrando información al sistema y quienes la digitan no tienen la suficiente capacitación para la manipulación del software por lo cual también se han generado inconvenientes para la muestra de informes, ejemplo claro de lo anterior se tiene que En la semana comprendida entre el 12 al 16 de mayo se desarrolló actividad de corrección de datos para los informes que presenta la Sra. Socorro Vallejo sobre la información Exógena, en ese proceso se observó que la información creada en el sistema sobre el TERCERO no es correcta. Se presentan errores como:

- Direcciones incompletas
- Nombres incompletos
- No saben diferenciar entre persona jurídica y natural
- No se especifica la ruta
- No se especifica el vendedor

Para lo anterior se sugiere a quien corresponda realizar una capacitación para la estandarización de la información, que el personal sepa cómo crear un TERCERO teniendo en cuenta los formatos correspondientes para esto, como es:

- La dirección debe tener como mínimo 8 caracteres
- Se deben utilizar las abreviaturas presentadas en el programa
- Se debe especificar cuando una persona es jurídica o natural
- El NIT siempre debe tener un código de verificación

Año tras año se ha venido presentando estos inconvenientes pero han sido corregidas únicamente en los formatos Excel para la Dian por lo cual el error se ha mantenido en el sistema. Si se corrige desde el software se evitara pérdida de tiempo en correcciones innecesarias.

El software SYSCAFE incluye la utilización de móviles como las pocket PC tipo PDA y actualmente móviles Nokia, este mecanismo ha ayudado a mejorar el proceso para registrar pedidos ya que se elimina el proceso de digitación de información mediante talonarios y se hace directamente en los móviles, DISPROPAN SAS cuenta con móviles tipo PDA y móviles Nokia los cuales actualmente se los está implementando y por lo cual también se han presentado inconvenientes en cuanto a la información que arroja y se sincroniza con GESTION

Se adecua el móvil PDA para trabajarse en la RUTA TUMACO con la ayuda de SYSCAFE, se realiza un manual de instrucciones para la persona encargada y se envía al responsable para que inicie a manejarlo el contrato de outsourcing del software: el contrato del software SISTEMA COMERCIAL SYSCAFE está debidamente legalizado y se cumple en su totalidad.

Plan de mejoramiento: con la realización de la auditoría se espera que esta genere un plan estratégico que asegure el manejo y control de la información concerniente a los INDICADORES DE FUNCIONAMIENTO DEL HARDWARE Y SOFTWARE EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO a fin de asegurar la calidad en la infraestructura tecnológica de la empresa DISPROPAN SAS y que mediante las vulnerabilidades encontradas se diseñe un plan de mejoramiento que permita mitigar los riesgos.

La realización de la auditoría aporta considerables beneficios a la empresa DISPROPAN SAS para la creación del área de sistemas, los principales son la mayor eficiencia en los procesos pertenecientes a esta área y a los procesos desarrollados con SYSCAFE, desarrollar un plan de mejoramiento que permita garantizar la seguridad, confiabilidad y disponibilidad de los recursos tecnológicos.

Se recomienda proporcionar orientaciones básicas para facilitar el proceso de la señalización de la localización de los medios de protección contra incendios, como la señalización de evacuación, salvamento y socorro en sus diferentes tipos y modalidades.

CONCLUSIONES

La Auditoría de Sistemas de Información, hoy en día es de vital importancia para las empresas modernas con visión de futuro, sobre todo inmersas en el mundo globalizado, porque si no se prevé los mecanismos de control, seguridad y respaldo de la información ésta se verá sumida a riesgos lógicos, físicos y humanos, que conlleven a fraudes no solamente económicos sino de información, es decir, pérdidas para la empresa, para ello toda empresa pública o privada deben de someterse a un control estricto de evaluación de eficiencia y eficacia con el objetivo de que los diferentes procesos funcionen correctamente.

Por medio de COBIT, el auditor logra entender la importancia de la seguridad de la información y de cómo se debe estar pendiente de esta seguridad, de que los sistemas y procesos funcionen correctamente para que cumplan con el objetivo por el cual fueron implementados.

Mediante el proceso de auditoría realizado en DISPROPAN SAS se logró determinar situaciones de debilidad en cuanto a la gestión de riesgos y seguridad física del hardware, manejo del software como también se identificó fortalezas en procesos de adquisición de infraestructura e indicadores de funcionamiento.

A pesar de que existen falencias en el manejo de la infraestructura tecnológica el personal encargado de cada una de las áreas de la empresa han demostrado un total sentido de pertenencia y están comprometidos con los procesos de mejoras, dependiendo también del apoyo que pueda brindar la alta gerencia.

Durante el desarrollo de la auditora es importante mencionar que dentro del análisis y observación se reparó que en DISPROPAN SAS no existen políticas para el análisis y la gestión de riesgos que permitan la identificación y clasificación de estos, También, hace falta realizar una revisión detallada de la red eléctrica, pues en las agencias se manifestó que hay inseguridad en la red eléctrica y se verifico mediante revisión visual, esta situación está afectando la seguridad de las personas y de los equipos pues se pueden provocar graves accidentes como incendios causados por sobrecarga eléctrica o descuido de cables sueltos o tendidos por el piso.

La realización de la auditoría aporta considerables beneficios a la empresa ya que mejora la eficiencia en los procesos pertenecientes al área de sistemas, desarrollar un plan de mejoramiento que permita garantizar la seguridad, confiabilidad y disponibilidad de los recursos tecnológicos, mediante los resultados obtenidos de la auditoría, entre otros.

Finalmente con la realización de la Auditoría se ha logrado que se hayan aplicado conocimientos y que como estudiante haya ampliado lo aprendido en las aulas de clases. Es importante la formación que se obtiene en la Universidad ya que uno se alimenta con el conocimiento y puede así alcanzar capacidades para analizar situaciones a los que se expone la información, identificando debilidades y fortalezas de los procesos que existen en una empresa, consiguiendo así mejorar la calidad de la información.

RECOMENDACIONES

Realizar planes de contingencia que permitan garantizar la continuidad de los servicio, ya que son claves para el correcto funcionamiento de los procesos que realizan en la empresa.

Crear un inventario tecnológico de los equipos de cómputo, servidores, entre otros con el fin de llevar un control y un registro adecuado de los activos de la empresa.

Capacitar al personal administrativo de la empresa en cuanto al manejo básico de un computador y de los programas ofimáticos.

Documentar un manual de funciones del personal que labora en la empresa.

Mejorar las instalaciones donde se encuentra el modem central de internet.

Mantener seguras las instalaciones del cableado de red de la empresa ubicando un gabinete.

Evaluar y estudiar el desempeño de la red de datos en su aspecto físico, teniendo en cuenta que hace falta una documentación adecuada de la red de datos.

Crear políticas y procedimientos relacionados con el estudio o análisis de nuevas tecnologías.

Realizar y Entregar al responsable de cada sede una copia del cronograma de actividades de mantenimiento con el fin de dar a conocer al personal de cada sede las fechas de mantenimiento con anterioridad para no afectar las actividades que se estén realizando en el momento de hacer el mantenimiento

BIBLIOGRAFIA

ARENS, Alvin A. Auditoría un Enfoque Integral. 6 Edición. México: Prentice Hall, 1996.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995

NETGRAFIA

http://www.dispropan.com.co
http://www.syscafe.com.co
http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n
http://es.wikipedia.org/wiki/COBIT
http://html.rincondelvago.com/auditoría-de-los-sistemas-de-informacion.html
http://www.slideshare.net/nelsyjazmin/diapositivas-1-7312584
http://www.monografias.com/trabajos14/auditoríasistemas/auditoríasistemas.shtml
http://cs.uns.edu.ar/~ece/auditoría/cobiT4.1spanish.pdf
http://www.eduardoleyton.com/apuntes/UDP_COBIT.pdf
http://www.definicion.org/auditoría-operacional