IMPLEMENTACION DE UNA AUDITORIA GENERAL EN LA SECRETARIA DE HACIENDA DE SABANAGRANDE

DE LA HOZ VALDIRIS ETHEL MARIA

PAUTH PALACIOS JAIR ALEXANDER

CORPORACIÓN UNIVERSIDAD DE LA COSTA (C.U.C.)
DEPARTAMENTO DE POSGRADO
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2012

IMPLEMENTACION DE UNA AUDITORIA GENERAL EN LA SECRETARIA DE HACIENDA DE SABANAGRANDE

DE LA HOZ VALDIRIS ETHEL MARIA

PAUTH PALACIOS JAIR ALEXANDER

CORPORACIÓN UNIVERSIDAD DE LA COSTA (C.U.C.)
DEPARTAMENTO DE POSGRADO
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2012

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Barranquilla, 10 de Diciembre de 2012

DEDICATORIA

Gracias a Dios por permitirme lograr una meta más en mi vida, por darme la luz para cumplir mis objetivos y llegar hasta el final.

Gracias a mi esposo BRIAN por su amor, apoyo incondicional y por sus palabras de aliento cuando era necesario.

Gracias a VALERY, DANIELA y SEBASTIAN por su comprensión y paciencia durante esta etapa y por motivarme a seguir adelante.

Gracias a mis docentes y compañeros de la especialización por todo su conocimiento, colaboración y apoyo.

ETHEL MARIA DE LA HOZ VALDIRIS

DEDICATORIA

Gracias a Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre Rosa por haberme apoyado en todo momento, por sus consejos y valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mi hermana Dayana por apoyarme en mis momentos difíciles, a mi tía Cleotilde, a mi tía Nelly y a todos aquellos que participaron directa o indirectamente en la elaboración de este trabajo de grado.

¡Gracias a ustedes!

A mis maestros por su gran apoyo y motivación para la culminación de este proyecto de grado

A mis amigos que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigo.

JAIR PAUTH PALACIOS

RESUMEN

Hoy en día las Entidades Públicas buscan mecanismos que le permitan asegurar y proteger el activo más valioso que se tiene como entidad, la Información. Debido a los altos riesgos que se enfrentan, se convierte en el punto más vulnerable y nace la idea de crear nuevas estrategias que nos permitan garantizar la seguridad de los sistemas, en el ambiente físico y brindar seguridad a la información que posee la Alcaldía Municipal de Sabanagrande.

De acuerdo con estas debilidades que presenta la entidad se propone la creación de nuevas estrategias de seguridad para satisfacer las necesidades presentada anteriormente. Estas ayudaran a que los procesos se manejen de una manera más segura, confiables y estén a la vanguardia de las nuevas tendencias en materia de innovación y/o implementación de TI, en la consecución de los objetivos trazados por la entidad y sus respectivas dependencia.

La Secretaria de Hacienda de Sabanagrande ha entendido que las falencias encontradas en el proceso de Recolección de Impuestos se ve reflejado en sus estados financieros y es por esto que nuestro equipo de Auditores tendrá la labor de analizar, evaluar los procesos y dar a los directivos mejoras y recomendaciones que ayuden a corregir las falencias encontradas.

Los conocimientos y experiencias obtenidos en el curso de la Especialización en Auditoria de Sistemas de la Información en la Corporación Universitaria de la Costa nos llevan a utilizar Los modelos ISO 27002 y COBIT 4.1 los cuales son normas internacionalmente aceptadas y los procesos y objetivos de Control utilizados, nos dan una visión amplia de los fallos que podemos encontrar en el proceso, nos sirven de guía para dar las recomendaciones para la continuidad del negocio permitiendo conocer, gestionar y minimizar los riesgos que atenten contra la seguridad de la información.

Además estas estrategias nos permitirán analizar, definir los procedimientos y controlar las medidas tomadas para proteger la información de la entidad.

ABSTRAC

Today, public entities are looking for tools that enable secure and protect the most valuable asset you have as an entity, The Information. Due to the high risks they face, becomes the most vulnerable and the idea to create new strategies that will guarantee the security of systems in the physical environment and provide security to the information held by the Municipality of Sabanagrande.

According to these weaknesses of the entity proposing the creation of new security strategies to meet the needs presented above. These help the processes are managed in a more secure, reliable and are at the forefront of new trends in innovation and / or implementation of IT in achieving the goals set by the entity and their dependence.

Treasury Secretary Sabanagrande understood that the shortcomings found in the Tax Collection process is reflected in its financial statements and that is why our team of auditors will have the task to analyze, evaluate processes and make improvements to management and recommendations to help correct the shortcomings.

The knowledge and experience gained in the course of Specialization in Audit of Information Systems at the University Corporation of Costa us to use models ISO 27002 and COBIT 4.1 whom are internationally accepted standards and processes and control objectives used give us a broad view of the fault to be found in the process, guide us to make recommendations for business continuity allowing knowledge, manage and minimize the risks that threaten the security of information.

Furthermore, these strategies will enable us to analyze, define procedures and control measures taken to protect information the entity.

CONTENIDO

Pág

LISTA DE IMÁGENES

Pág.

INTRODUCCIÓN

En la actualidad llevar a cabo una auditoría a los procesos que no están alcanzando los resultados esperados es la mejor opción, después de realizar una respectiva evaluación, para luego dar una serie de recomendaciones que ayuden a minimizar las falencias y riesgos encontrados, que nos puedan estar afectando a la consecución de los objetivos propuestos para dicho proceso.

El presente trabajo busca implementar un adecuado conjunto de controles y recomendaciones a los procesos, procedimientos, y funciones de software y hardware auditado, para tratar de Minimizar cada unas de las vulnerabilidades encontradas en la dependencia de la Secretaría de Hacienda del Municipio de Sabanagrande.

Esta dependencia es responsable de la Administración Financiera y Tributaria del Municipio, en la cual se encarga de asegurar la eficaz y honesta obtención y administración de Los recursos en un marco de legalidad y justicia, vigilando la estricta aplicación de los recursos financieros del municipio para garantizar su aplicación conforme a los objetivos trazados, corrigiendo desviaciones cuando se presentan.

Para llevar a cabo esta auditoria en la secretaría de hacienda del municipio de Sabanagrande, se han establecido como objetivo identificar información y controles existente, realizar el análisis de evidencia recaudada para emitir recomendaciones a los riesgos encontrados para mejorar los controles físicos y controles de aplicación, para asegurar y garantizar la confidencialidad de la información, que se verán reflejados en el buen manejo administrativo por parte de los funcionarios que laboran en dicha dependencia.

1. PLANTEAMIENTO DEL PROBLEMA

Las entidades públicas cada día requieren mejorar los procesos de cada área o dependencia con las que cuentan, por lo que se verá enfrentada a ciertos retos que tendrá que sobrepasar. Entre estos retos, se encuentra la seguridad de la información en la dependencia de la secretaría de hacienda, tarea que no es fácil si no hay organización y controles adecuados, para lo cual se debe tener al personal de esta dependencia altamente capacitado para lograr la consecución de los objetivos propuestos.

Unas de las problemática que se dan en la dependencia de la secretaría de hacienda es que no cuentan con la adecuada infraestructura tecnológica para agilizar los procesos de manera eficiente, esta auditoria permitirá identificar en la Oficina de la Secretaría de Hacienda cuales son las falencias en la seguridad de los sistemas, administración de los datos y del ambiente físico y se tomará como marco de referencia el modelo COBIT y el estándar internacional ISO 27002.

Se realizaran visitas a la secretaria de hacienda entrevistando a los funcionarios de esta dependecia, observando los procedimientos de almacenamiento de los datos previo y posterior al recaudo de los recursos finacieros y validando los soportes digitales con los soportes fisicos.

2. JUSTIFICACIÓN

En el municipio de Sabanagrande, por medio de la Secretaria de Hacienda, se recaudan los impuestos municipales, los cuales le representan un ingreso sustancial a la alcaldía municipal para el cumplimiento de las metas propuestas por el consejo administrativo, en busca de lograr sus objetivos de acuerdo al presupuesto establecido a cumplir.

Después de que se realiza el cobro y se recaudan los impuesto, la secretaria de hacienda adquiere información que es de tipo confidencial, información que de inmediato debe tener unos parámetro de seguridad, desde su entrada al sistema hasta su almacenamiento en el archivador, cumpliendo los procedimientos establecido por las normas ISO 27002 y COBIT 4.1.

2.1 BENEFICIOS ORGANIZACIONALES

Este proyecto fue realizado con el fin de brindarle, a la Secretaria de Hacienda del Municipio de Sabanagrande, seguridad y confiabilidad en la informacion durante el cumpliento de los procedimientos exigido por el gobierno, mediante las normas de seguridad de informacion como son la ISO 27002 y Cobit.

2.2 BENEFICIOS ECONÓMICOS

Las entidades publicas colombianas deberia implementar mas oportunamente estos estandares y|o normas con el fin de proteger, su activo mas valioso, la informacion. La proteccion de este activo se vera reflejado en la inversion social, teniendo en cuenta que las entidades públicas buscan herramientas eficientes casi que a diario para tratar de recaudar la mayor cantidad de ingresos posibles con el fin de brindarles un mejor bienestar a todo los habitantes, ya sea por convenios con otras entidades o por proyecto que ayuden a mejorar la calidad de vida de la comunidad y proporcionen un buen desarrollo a los municipios, se hace necesario aprovechar al máximo la

oportunidad que ha brindado la Corporación Universitaria de la Costa C.U.C, para plantear la siguiente propuesta: **IMPLEMENTACION DE UNA AUDITORIA GENERAL EN LA DEPENDECIA DE LA SECRETARIA DE HACIENDA DE SABANAGRANDE.**

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar una Auditoria que permita garantizar la seguridad de la información en la dependencia de la secretaría de hacienda del municipio de Sabanagrande, creando una cultura de protección, integridad y confidencialidad de la información en la dependencia.

3.2 ESPECÍFICOS

- Identificar la información confidencial de la secretaría de Hacienda Distrital
- Identificar los controles existentes enfocados a la seguridad de la Secretaría de Hacienda.
- Verificar la seguridad de las aplicaciones (métodos de control de acceso, confiabilidad y respaldos).
- Verificar los datos obtenidos mediantes los procedimientos establecidos por el software de registros de impuestos en el municipio de Sabanagrande.
- Realizar recomendaciones pertinentes a los riesgos encontrados para mejorar los controles físicos y controles de aplicación.

4. DELIMITACIÓN

4.1 DELIMITACIÓN ESPACIAL

El periodo de Auditoria se realizará en la Secretaria de Hacienda del Municipio de Sabanagrande, ubicada en Dirección: Carrera 7 Nº 5 -10, Primer Piso Alcaldía Muncipal de Sabanagrande – Atlantico, Colombia

4.2 DELIMITACIÓN TEMPORAL

El periodo de Auditoria se llevará a cabo en un lapso máximo de 8 meses, el cual inicio el de 14 de Agosto de 2011 y finalizo el 25 de Abril del año 2012.

4.3 DELIMITACIÓN TÉCNICA

Para este proyecto se hizo uso de las siguientes normas y estándares:

- COBIT 4.1
- ISO 27002:2005

5. MARCO TEORICO

En el municipio de Sabanagrande, por medio de la Secretaria de Hacienda Municipal, se debe recaudar el impuesto predial anualmente, lo cual le representara un ingreso sustancial a la Alcaldía Municipal para el cumplimiento de las metas propuestas por el consejo administrativo, en busca de lograr sus objetivos de acuerdo al presupuesto establecido a cumplir.

Las correcciones de las fallas presentes en la seguridad de los sistemas, administración de datos y ambiente físicos serán una oportunidad para que la Alcaldía de Sabanagrande alcance las metas propuestas en su proceso de Recolección del Impuesto Predial.

Para la realización de este trabajo el equipo de Auditores no encontró auditorías realizadas anteriormente por lo cual nos hemos basado en la Norma ISO 27002 y en COBIT para hallar debilidades y presentar sugerencias de mejoras al proceso.

Los objetivos de control específicos utilizados en esta Auditoria son:

- DS5 Garantizar la Seguridad de los Sistemas
- DS11 Administrar los Datos
- DS12 Administrar el Ambiente Físico

Basaremos nuestra Auditoria en estos Objetivos de Control para que el Departamento de la Secretaría de Hacienda de la Alcaldía de Sabanagrande implemente soluciones que le permitan Garantizar la seguridad de los Sistemas, Mejorar la Administración de los Datos y el Ambiente Físico.

5.1 COBIT

COBIT (Control Objectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada) es un marco de referencia mundialmente aceptado para el gobierno y gestión de las tecnologías de la información. Fue desarrollado por la Information Systems Audit and Control Association (ISACA) en asocio con el IT Governance Institute (ITGI).

Este marco de referencia ofrece un conjunto de mejores prácticas para garantizar la alineación de las tecnologías de la información con los objetivos del negocio, el uso eficiente de los recursos tecnológicos, la administración adecuada de los riesgos y el aumento de los beneficios del negocio mediante el uso de las tecnologías de la información.

De igual forma, define como responsables del gobierno de tecnologías de la información a la junta directiva y ejecutivos de la organización. Así mismo, define 5 áreas de enfoque en las cuales los ejecutivos deben colocar atención para realizar una adecuada gobernabilidad de las tecnologías de la información (Figura 1).

Figura 1. Áreas de enfoque de Gobierno de TI

COBIT tiene como misión “Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales

de aseguramiento."[1] y se basa en el siguiente como principio "Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida"[2] (Figura 2).

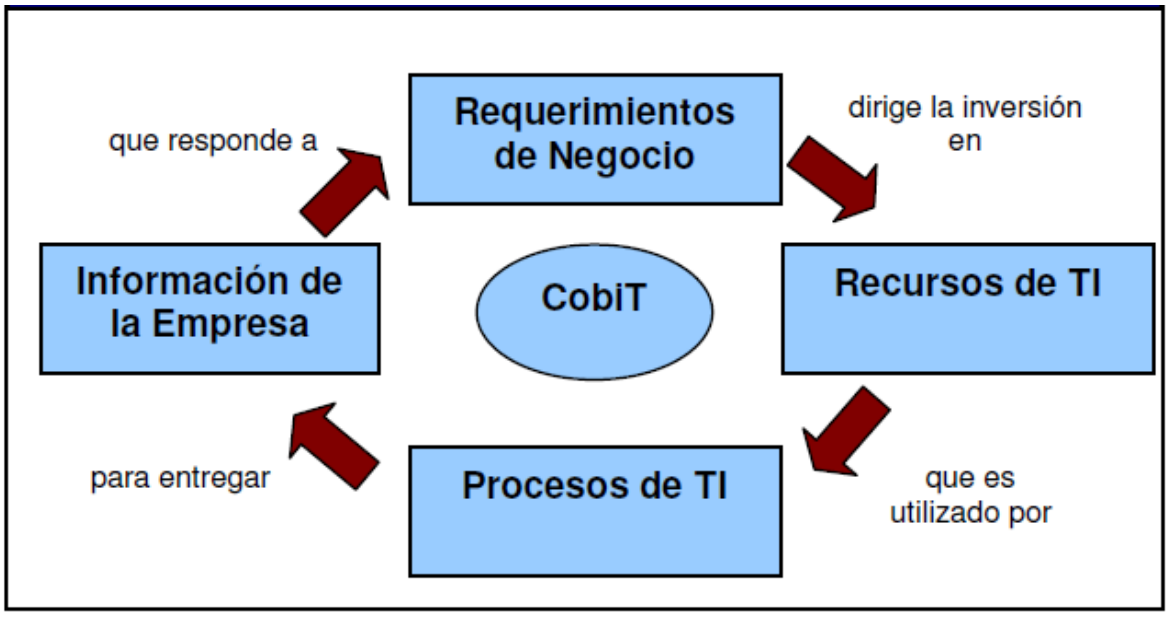


Figura 2. Principios Básicos de COBIT

Para el cumplimiento de los requerimientos de la organización COBIT define recursos de tecnologías de la información en los cuales la organización debe invertir y velar por su buen funcionamiento. Estos recursos son:

Las personas: compuesto por el recurso humano necesario para gestionar los servicios y recursos de TI.

La infraestructura: compuesto por el Hardware y software que soportan las aplicaciones.

La información: compuestos por los datos en todas sus formas, ingresados, procesados o generados por los sistemas de información.

[1] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICION, 2007. Pág. 13
[2] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICION, 2007. Pág. 14

Las aplicaciones: compuestos por sistemas automatizados y procedimientos manuales para el procesamiento de información.

Para la consecución de los objetivos de la organización COBIT define 7 criterios que la información debe cumplir estos son:

Eficiencia: la información debe ser generada de manera óptima.
Efectividad: la información debe ser pertinente y relevante para la organización.
Confidencialidad: la información sensible de la organización debe ser conocida y manipulada por personal autorizado.
Integridad: la información deber ser precisa, completa y exacta.
Disponibilidad: la información debe estar disponible en el momento en que cualquier proceso de la organización lo requiera.
Cumplimiento: la información debe satisfacer las regulaciones y leyes aplicables a la organización
Confiabilidad: la información entregada a la alta gerencia debe ser apropiada.

Para gobernar adecuadamente TI se deben establecer actividades y procedimientos que deben ser gestionados, COBIT agrupa estas actividades en 4 dominios, que son:

Planear y Organizar: en este dominio se cubre todo lo referente a la alineación de las tecnologías de la información con los objetivos del negocio. Definiendo una estrategia que permita a la organización hacer uso de los recursos tecnológicos en pro del óptimo funcionamiento de sus procesos. Se subdivide en 10 procesos:

- 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

Adquirir e Implementar: este dominio cubre la identificación, adquisición, implementación y mantenimiento de las soluciones y recursos de TI necesarios para el cumplimiento del plan estratégico de TI. Se subdivide en 7 procesos:

- 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

Entregar y Dar soporte: este dominio cubre la entrega de los servicios requeridos por la organización y el soporte de las aplicaciones y recursos de TI en general. Se subdivide en 13 procesos:

- 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
- DS7 Educar y entrenar a los usuarios

- DS6 Identificar y asignar costos
- 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

Monitorear y Evaluar: este dominio cubre la revisión continua y administración del desempeño de los recursos de TI. Así como el monitoreo y evaluación del control interno, el cumplimiento de las regulaciones aplicables a la organización y la administración del gobierno de TI. Se subdivide en 4 procesos:

- 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

COBIT cuenta con un modelo de madurez compuesto por 6 Niveles que van de 0 a 5 (Figura 3). Este modelo permite evaluar el nivel de cumplimiento de la organización con respecto a los objetivos de control que esta haya adoptado. Cada uno de los procesos de COBIT puede ser evaluado a través de este sistema dando como resultado las condiciones actuales de la organización, lo que le permitirá realizar comparaciones con sus organizaciones de su mismo entorno. De igual forma, le permitirá a la organización elegir el nivel de madurez en el que desea estar a futuro y determinar la brecha entre su estado actual y el deseado. A partir de estos resultados la organización definirá la estrategia y procedimientos a seguir para llegar a su estado deseado.

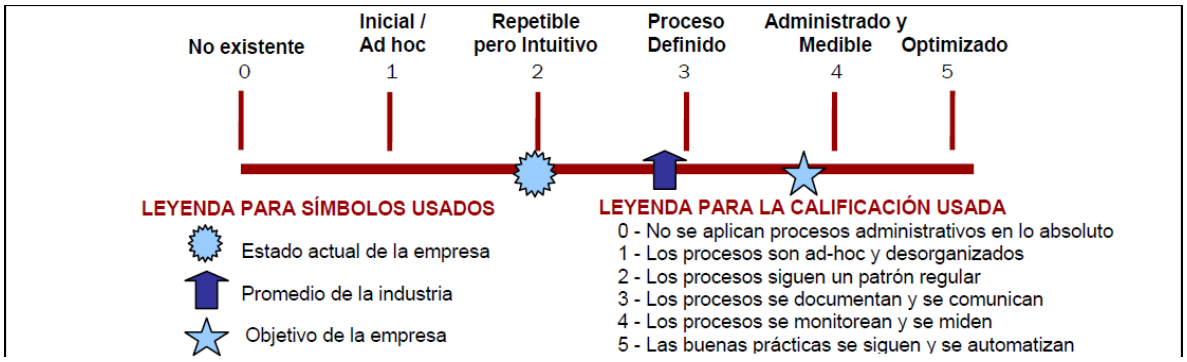


Figura 3. Representación Gráfica Del Modelo De Madurez COBIT

DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS [3]

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

Control sobre el proceso de TI de garantizar la seguridad de los sistemas que satisface el requerimiento del negocio de TI para mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

Enfocándose en la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.

[3] COBIT. IT GOVERNANCE INSTITUTE.CUARTA EDICIÓN, 2007. Pág 124

Se logra con:

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular.

Se mide con:

- El número de incidentes que dañan la reputación con el público.
- El número de sistemas donde no se cumplen los requerimientos de seguridad.
- El número de violaciones en la seguridad de las tareas.

Objetivos de Control

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 negocios, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas, desarrollo y mantenimiento) deben ser identificados 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 o 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. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y Monitoreo de la Seguridad

Garantizar que la implementación de la seguridad de TI sea aprobada y monitoreada de forma proactiva. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

DS5.6 Definición de Incidente de seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

DS5.7 Protección de la Tecnología de Seguridad

Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

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 implementadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizada.

DS5.9 Prevención, Detección y Corrección de software malicioso

Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware.

DS5.10 Seguridad de la red

Uso de técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos Sensitivos

Transacciones de datos sensibles de intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no de repudio de origen.

DS11 ADMINISTRACIÓN DE DATOS [4]

Una efectiva administración de los datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la

[4] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICIÓN, 2007 Pág 148

eliminación apropiada de medios. Una afectiva administración de datos y la eliminación apropiada de medios. Una afectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

Administración de datos que satisface el requerimiento del negocio de TI para optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera. Enfocándose en mantener la integridad, exactitud, disponibilidad y protección de los datos.

Se logra con:

- Respaldando los datos y probando la restauración.
- Administrando almacenamiento de datos en sitio y fuera de sitio.
- Desechando de manera segura los datos y el equipo

Y se mide con:

- Satisfacción del usuario con la disponibilidad de los datos.
- Porcentaje de restauraciones exitosas de datos.
- Número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados.

Objetivos de Control

DS11.1 Requerimientos del Negocio para Administración de Datos

Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos del negocio. Las necesidades de reinicio y reproceso están soportadas.

DS11.2 acuerdos de almacenamiento y control

Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.

DS11.3 SISTEMA DE ADMINISTRACION DE LIBRERIAS DE MEDIOS

Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.

DS11.4 ELIMINACIÓN

Definir e implementación asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

DS11.5 RESPALDO Y RESTAURACIÓN

Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.

DS11.6 REQUERIMIENTOS DE SEGURIDAD PARA LA ADMINISTRACIÓN DE DATOS

Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibir procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios.

DS12 ADMINISTRACIÓN DEL AMBIENTE FISICO [5]

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

[5] COBIT. IT GOVERNANCE INSTITUTE. CUARTA EDICIÓN, 2007 Pág 152

Administración del ambiente físico que satisface el requerimiento del negocio de TI para proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio. Enfocándose en proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.

Se logra con:

- Implementando medidas de seguridad físicas.
- Seleccionando y administrando las instalaciones.

Y se mide con:

- Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico.
- Número de incidentes ocasionados por fallas o brechas de seguridad física.
- Frecuencia de revisión y evaluación de riesgos físicos.

Objetivos de Control

Ds12.1 Selección y Diseño del Centro de Datos

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

Ds12.2 Medidas de Seguridad Física

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

Ds12.3 Acceso Físico

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

Ds12.4 protección Contra Factores Ambientales

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

Ds12.5 Administración de Instalaciones Físicas

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

5.2 ISO 27002

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la comisión Electrotécnica Internacional (IEC).

ISO 27002 Es la norma es la norma que contiene los requisitos del sistema de seguridad de la información. Esta norma en su anexo A enumera objetivos de control y controles que podrán seleccionar las organizaciones para la creación de su sistema de seguridad de la información. Estos objetivos se encuentran ampliamente desarrollados en la ISO 27002, no todos son de obligatorio cumplimiento ya que depende de las condiciones del negocio. Sin embargo el no cumplimiento de un objetivo de control debe ser justificable.

Estas normas permiten gestionar la seguridad de la información y por consiguiente la continuidad de los procesos en la que esta es participe en cualquiera de sus estados.

6. DISEÑO METODOLÓGICO

6.1 TIPO DE DISEÑO

Descriptivo: Porque permite medir, evaluar o recolectar datos sobre diversos aspectos, dimensiones o componentes de la investigación que se va a realizar. Esto con el fin de recolectar toda la información que obtengamos para poder llegar al resultado de la investigación.

6.2 MÉTODO DE ESTUDIO

El método de estudio que se llevará a cabo es por Observación.

6.3 TÉCNICA DE RECOLECCIÓN DE INFORMACIÓN

6.3.1 Técnica de Recolección de la Información Primaria. Se trabajara con la observación directa producto de la realidad**.**

6.3.2 Técnica de Recolección de la Información Secundaria Se recolecto información del marco de referencia COBIT 4.1, la norma ISO 27002, y se trabajo con las fuentes de segunda mano tales como, revistas, Internet.

6.4 INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

- **Instrumento de Recolección de la Información Primaria** El instrumento a utilizar es la Lista de Chequeo.

- **Instrumento de Recolección de la Información Secundaria** Como instrumento de recolección de información secundaria el trabajo se apoyo en los siguientes estándares, buenas prácticas, normas, y/o guías:
  - ISO 27002
  - COBIT 4.1

7. RECURSOS DISPONIBLES

7.1 RECURSOS MATERIALES

Biblioteca
Acceso a Internet
COBIT 4.1
Norma ISO: 27002
Equipo de Cómputo 3

7.2 RECURSOS FINANCIEROS

Transporte local	180.000
Papelería	50.000
Servicio de Internet	90.000
Otros	170.000
TOTAL	**$ 490.000**

8. PLAN DE TRABAJO

Este proyecto permite a la SECRETARIA DE HACIENDA MUNICIPAL DE SABANAGRANDE, identificar y tener un conocimiento más claro de las distintas vulnerabilidades con las que cuentan hoy día en su plataforma tecnología y la seguridad de la información critica, por ello en la elaboración de este trabajo de grado se utilizan diferentes estándares que se consideran como las mejores prácticas para tales fines

Primero que todo hacemos una presentación ante el Secretario de Hacienda de lo que pretendemos con el proyecto, Luego se hace una ambientación por parte del secretario de hacienda de cómo funciona las instalaciones de la Secretaria de Hacienda Municipal para establecer con mayor claridad los procesos que allí se desarrollan, Después de entrevistar al Secretario de Hacienda y a los empleados ellos expresaron sus inquietudes y preocupaciones respecto a las vulnerabilidades que se vienen presentando en la infraestructura tecnológica y la seguridad de la información.

Después de haber identificado los riesgos y las vulnerabilidades que la Secretaria de Hacienda presenta, el equipo de trabajo de auditores se encargo de detectar las falencias de mayor criticidad que tiene la Secretaria de Hacienda con el fin de darles las recomendaciones pertinentes y de esta manera minimizar el impacto de las amenazas. Esto se logro tomando como base de referencia el estándar COBIT 4.1 e ISO 27002.

Para terminar el trabajo llevado a cabo por el equipo de auditores ellos presentaran un informe final a la Secretaria de Hacienda Municipal con la finalidad de que ellos tomen conciencias de las vulnerabilidades que presentan y a través de estas recomendaciones tomar las respectivas medidas para mejorar los procesos en los que actualmente están fallando en dichas dependencias.

9. ENTREGA DE PROPUESTA DE AUDITORIA

Después de haber llevado a cabo la respectiva identificación de los puntos a tratar y de las vulnerabilidades a corregir, el equipo de trabajo planteo unas recomendaciones donde se plasmaba el compromiso por parte del equipo hacia la Secretaria de Hacienda Distrital de Sabanagrande.

A continuación se muestra la propuesta entregada por los auditores:

SECRETARIA DE HACIENDA DISTRITAL DE SABANAGRANDE

Barranquilla. Febrero 10 del 2012

Señor
Osvaldo Barrios De la Cruz
Secretario de hacienda y del Tesoro
Municipio de Sabanagrande

REF:

De acuerdo al plan de auditoría, damos inicio a la auditoria en referencia, en el periodo comprendido del 10 de agosto al 30 de noviembre del año anterior, la cual será desarrollada por los auditores:

Ethel María De la Hoz Valdiris
Jair Pauth Palacios

A continuación describimos los objetivos y alcance de esta auditoría:

Objetivos.

- Identificar la información confidencial de la secretaría de hacienda distrital
- Identificar los controles existentes enfocados a la seguridad de la secretaría de hacienda.
- Verificar la seguridad de las aplicaciones (métodos de control de acceso, confiabilidad y respaldos).
- Verificar los datos obtenidos mediantes los procedimientos establecidos por el software de registros de impuestos en el municipio de Sabanagrande.
- Realizar recomendaciones pertinentes a los riesgos encontrados para mejorar los controles físicos y controles de aplicación.

Alcance

Para la realización de la siguiente auditoria se tuvo en cuenta los siguientes aspectos:

- Análisis de riesgos en la plataforma tecnológica de la Secretaria de Hacienda.
- Evaluación del acceso lógico al software y archivos
- Verificación de existencia de políticas de Backup y recuperación de información confidencial.

CRONOGRAMA DE ACTIVIDADES RECAUDO IMPUESTO DE SABANAGRANDE

		MES 1			MES 2				MES 3				MES 4				MES 5			
Actividad	**Responsable**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Presentación de la Auditoria	Ethel De la Hoz Jair Pauth																			
Conocimiento de las instalaciones de la secretaría de Hacienda	Ethel De la Hoz Jair Pauth																			
Entrega propuesta de Auditoria	Ethel De la Hoz Jair Pauth																			
Identificación de Riesgos	Ethel De la Hoz Jair Pauth																			
Identificación de Controles Existentes	Ethel De la Hoz Jair Pauth																			
Evaluar controles existentes	Ethel De la Hoz Jair Pauth																			
Identificar y proponer opciones de tratamiento	Ethel De la Hoz Jair Pauth																			
Preparar informe de Auditoria	Ethel De la Hoz Jair Pauth																			
Entrega de informe final de Auditoria	Ethel De la Hoz Jair Pauth																			

10.2 IDENTIFICACION DE RIESGOS

Riesgo: Es el costo o valor de las perdidas que sufre o se expone a sufrir una organización, como consecuencia a las manifestaciones de situaciones no deseadas denominadas causas o amenazas de riesgo y efectos. Considerando lo perjudicial que puede ser para la Secretaria de Hacienda Distrital del Municipio de Sabanagrande que se materialice algunos de los riesgo que dicha dependencia presenta, nuestro equipo de auditores se encargo de identificar los riesgos de mayor impacto, utilizando los diferentes métodos aprendidos durante la especialización y dejando evidencias inmediatas que reflejan la veracidad y existencia de las fallas encontradas.

A continuación se muestran los riesgos de la plataforma física de la Secretaria de Hacienda Distrital con sus respectivas evidencias y recomendaciones para su solución.

DESARROLLO DE LA AUDITORÍA

9.3 ADMINISTRACION DEL AMBIENTE FISICO

9. Seguridad Física y Ambiental

- Pérdida, daño o robo de la información por falta de controles de accesos al permitir el ingreso al personal no autorizado en el área de centro de cómputo.

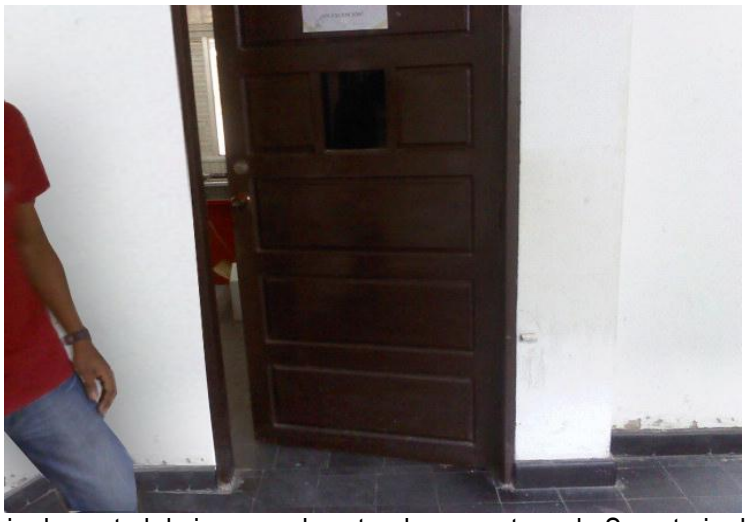


Imagen 4. Ausencia de control de ingreso al centro de computo en la Secretaria de Hacienda

La vulnerabilidad anteriormente detectada está violando los siguientes objetivos de control que hacen parte de ISO 27002 y COBIT 4.1

- **Objetivos de control ISO 27002**

9. Seguridad física y del entorno
9.1 Áreas seguras
9.1.1 Perímetro de seguridad física
9.1.2 Controles de acceso físico
9.1.3 Seguridad de oficinas, despachos e instalaciones
9.2 Seguridad de los equipos

- **Objetivos de control COBIT**

DS12.3 Acceso Físico

- Daño o deterioro de los equipos de cómputo por falta de un debido mantenimiento preventivo del cableado eléctrico.

Imagen 6. Ausencia de protección correcta en el cableado

Las vulnerabilidades anteriormente detectadas están violando los siguientes objetivos de control que hacen parte de ISO 27002 y COBIT 4.1

- **Objetivos de control ISO 27002**

9.2.1 Ubicación y protección del equipo
9.2.3 Seguridad en el cableado.

- **Objetivos de control de COBIT 4.1**

DS 12.4 Protección contra factores Ambientales
DS 12.5 Administración de instalaciones físicas

10. Gestión De Comunicaciones Y Operaciones

- Pérdida o modificación de la información crítica en el software Transfor debido a la ausencia de segregación de funciones de los funcionarios que laboran en la Secretaría de Hacienda.

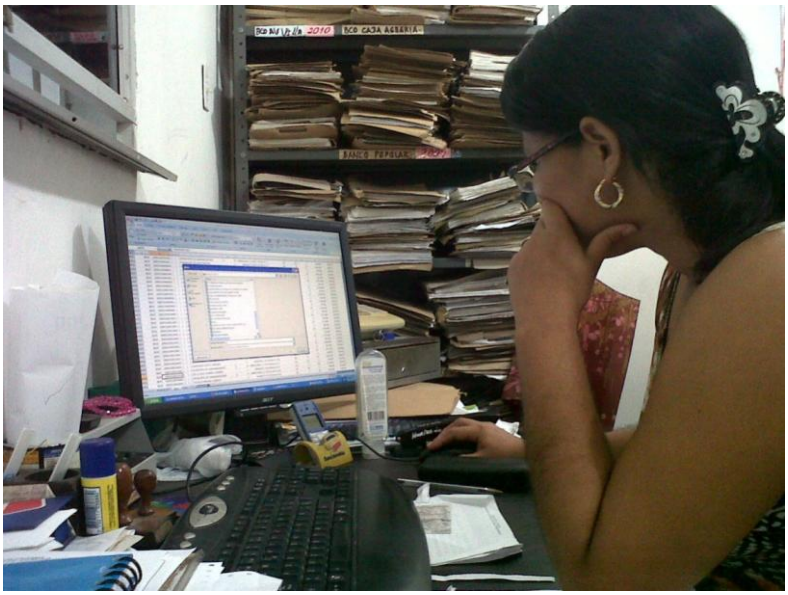


Imagen 8. Ausencia de control en la segregación de funciones

La vulnerabilidad anteriormente detectada esta violando los siguientes objetivos de control que hacen parte de ISO 27002 y COBIT 4.1

- **Objetivos de control ISO 27002**

10.1.3 Distribución (segregación) de funciones

- **Objetivos de control COBIT 4.1**

PO4.11 Segregación de funciones

9.4 SEGURIDAD DE LOS SISTEMAS

- Ingreso no autorizado al sistema por ausencia de clave en la cuenta de usuario

Imagen 9. Ingreso no autorizado al sistema

La vulnerabilidad anteriormente detectadas en el equipo de cómputo, están violando los siguientes objetivos de control que hacen parte de ISO 27002 y COBIT 4.1

- **Objetivos de control ISO 27002**

11.5 Control del acceso al sistema operativo
11.5.1 Procedimientos para un registro seguro

- **Objetivos de control COBIT 4.1**

DS5. Garantizar la seguridad de los sistemas
DS5.4 Administración de cuentas de usuario

- Acceso a la información importante de la secretaría de hacienda por falta de seguridad en las aplicaciones y archivos compartidos por los funcionarios.

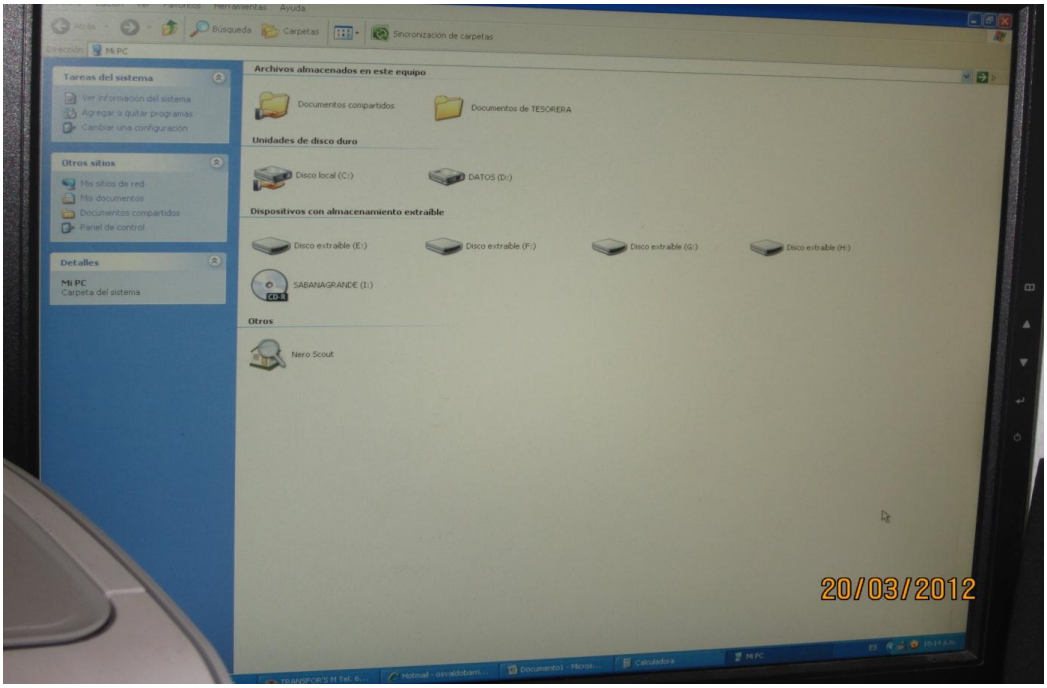


Imagen 10. Manejo sin control de la información contenida en Carpetas y discos duros compartidos

Imagen 11. Manipulación del software de impuesto predial sin clave de seguridad.

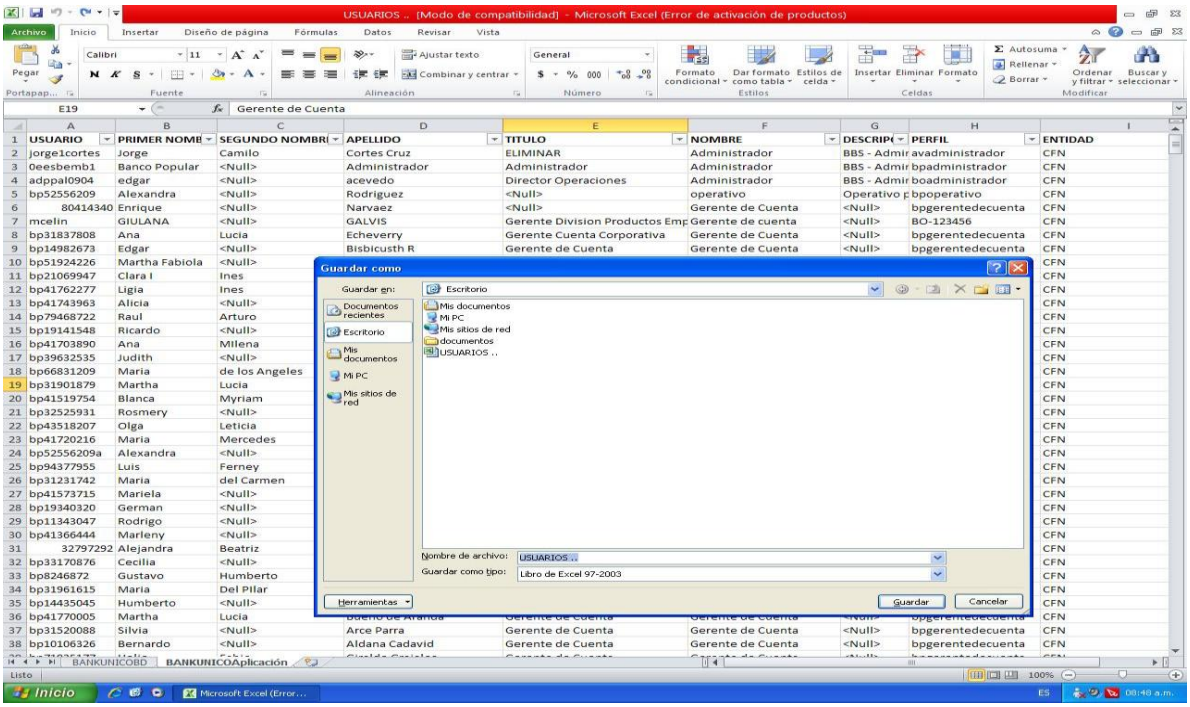


Imagen 12. Manipulación de la información almacenada en la base de datos por parte de varios funcionarios

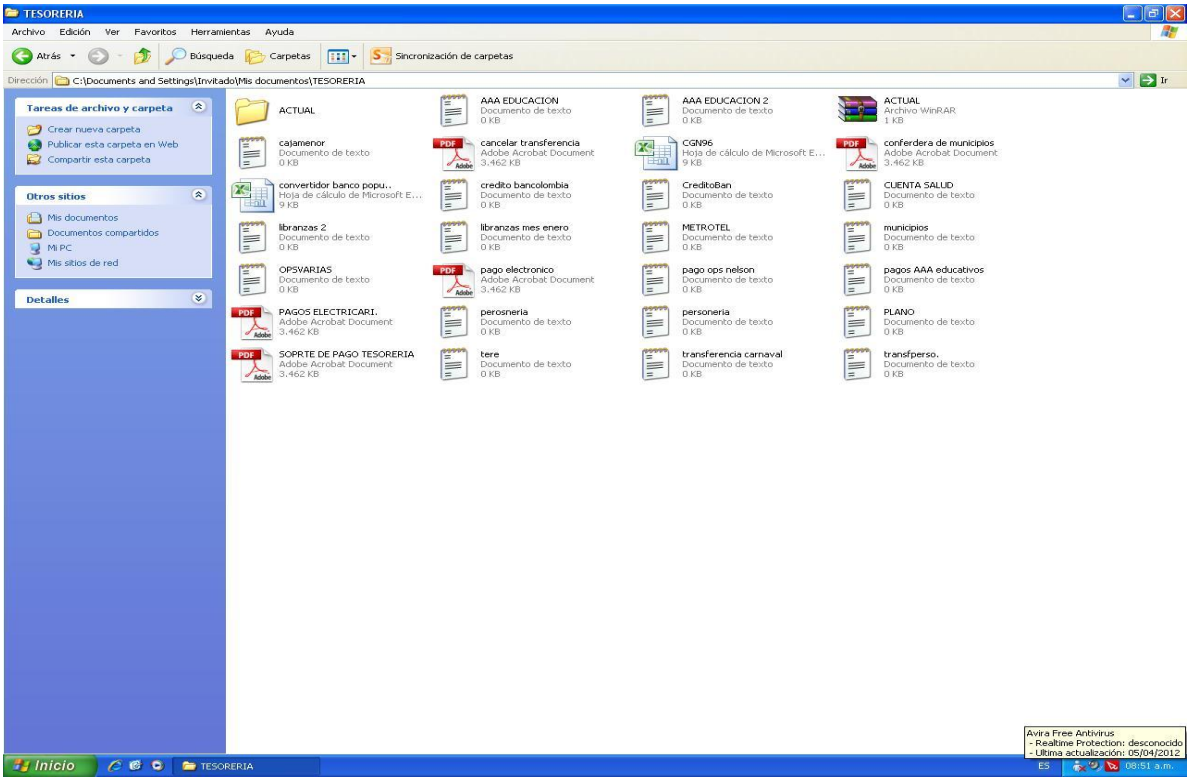


Imagen 13. Ausencia de activación del antivirus

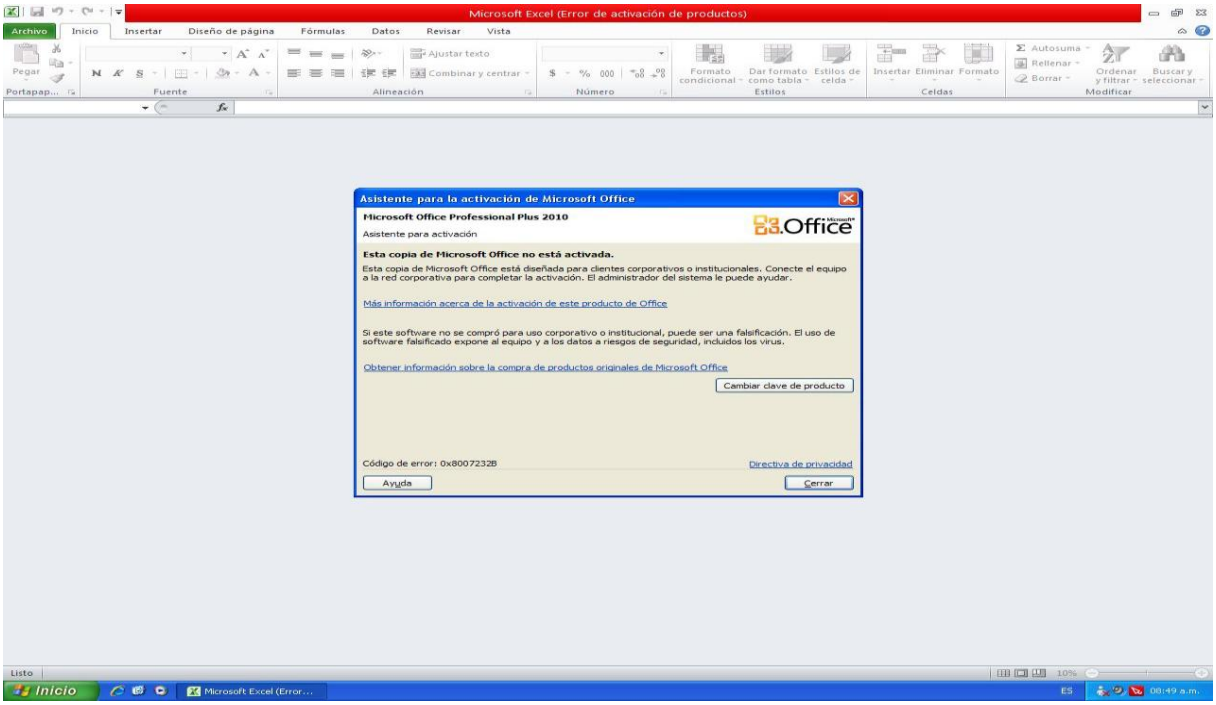


Imagen 14. Ausencia de activación del paquete de Microsoft office

Las vulnerabilidades anteriormente detectadas en el equipo de cómputo donde se lleva a cabo en el proceso de impuesto predial, están violando los siguientes objetivos de control que hacen parte de ISO 27002 y COBIT 4.1

- **Objetivos de control ISO 27002**

10.4 Protección contra el código malicioso y móvil
11.5 Control del acceso al sistema operativo
11.6 Control de acceso a la aplicación y la información
11.6.1 Restricción del acceso a la información
12.4 Seguridad de los archivos del sistema

- **Objetivos de control COBIT 4.1**

DS5. Garantizar la seguridad de los sistemas
DS5.4 Administración de cuentas de usuario
DS5.9 Prevención, Detección y Corrección de software malicioso

10. ENTREGA DE INFORME FINAL DE AUDITORIA

Barranquilla, Octubre 10 de 2011

Señor
OSVALDO BARRIOS DE LA CRUZ
SECRETARIO DE HACIENDA Y DEL TESORO
Municipio de Sabanagrande
E. S. M.

Ref: Informe con los resultados de la Auditoría a la Secretaria de Hacienda Distrital de Sabanagrande, Infraestructura Física, Tecnológica.

Cordial saludo,

Nos complace presentar a su consideración el informe con los resultados de la Auditoría de Sistemas efectuada.

1. OBJETIVOS Y ALCANCE DE LA AUDITORIA

La auditoría tuvo como objetivo evaluar el grado de apoyo de los sistemas informáticos llevado a cabo en la Secretaria de Hacienda, evaluar y verificar los procedimientos de seguridad y controles utilizados en el proceso recaudo del impuestos, e incluyo la evaluación y verificación de los controles en la generación y entrada de datos, procesamiento, documentación y calidad de la información producida.

La auditoría enfatizó en los controles necesarios para minimizar la probabilidad de ocurrencia de los cuatro (4) riesgos potenciales resultantes como críticos en el Análisis de Riesgos efectuado: Pérdida de Ingresos, Fraude, Pérdida de Credibilidad Pública, Decisiones Erróneas.

En nuestra revisión evaluamos y verificamos los controles en los siguientes procesos de la aplicación:

- ✓ Generación y Entrada de Datos
- ✓ Procesamiento y Actualización de Datos
- ✓ Seguridad y Calidad de la Información Generada
- ✓ Acceso Lógico al Software y Archivos
- ✓ Documentación del Sistema
- ✓ Políticas de Backup y Recuperación de información confidencial.

2. METODOLOGIA EMPLEADA

La Auditoría se desarrollo de acuerdo con las normas de auditoría generalmente aceptadas, especialmente las promulgadas para la Auditoría de Sistemas de Información por ISACA (Information Systems Audit and Control Association, Inc).

Para satisfacer los objetivos de la auditoría se desarrollaron los siguientes pasos y procedimientos:

a. Se efectuaron entrevistas con la funcionaria Liliana Carrillo, auxiliar contable, encargada de algunos procesos de administración del sistema de recaudo y Osvaldo Barrios, secretario de hacienda del municipio Sabanagrande.

b. Con base en las vulnerabilidades que evidenciamos se inició el proceso de auditoría, enfatizando en los riesgos críticos detectados. Este proceso consistió en a) Identificar las causas de los riesgos críticos. b) Identificar y evaluar los controles utilizados. c) Diseñar y ejecutar las pruebas de auditoría alrededor y a través de los equipos de computo y d) Elaboración y presentación del informe con los resultados de la Auditoría.

3. RESULTADOS DE LA AUDITORIA

3.1. OPINION DE LA AUDITORIA

- El nivel de riesgo por fraude o perdida de información es alto debido a que no cuentan con un control restrictivo para el uso de la cuenta de administrador, ni la definición de cuentas de usuario.

- Los procedimientos y controles internos relativos a los procesos de Recaudos, en gran parte están definidos por la propia mecánica del Sistema de Información TRANSFOR, sin embargo no se encuentran formalmente documentados, lo cual los torna en ocasiones informales y vulnerables a modificaciones no autorizadas.

- En la Estructura Organizativa de la Unidad existe un alto grado de compromiso y dedicación, sin embargo amerita ser revisada en lo concerniente a una apropiada segregación de funciones.

- No obstante la seguridad de los sistemas es deficiente, debido básicamente a los altos privilegios de acceso, sobre el Sistema Operacional, otorgados a los usuarios y que son consecuencia de una inadecuada definición de perfiles en el sistema operacional.

  De igual manera la inexistencia de una política para la periodicidad en la realización de las copias de seguridad, contribuye desfavorablemente al riesgo de pérdidas de confiabilidad, integridad y disponibilidad de la información.

3.2. PRINCIPALES RECOMENDACIONES Y PUNTOS A MEJORAR

Administración del ambiente físico

- Todos los empleados de la secretaría de Hacienda Distrital de Sabanagrande deben recibir formación adecuada en concientización de la seguridad de la información.
- Deben instalarse equipos y dispositivos especializados de acuerdo a las necesidades de la entidad para monitorear y controlar el ambiente.
- Se deberían instalar extintores en el área donde se encuentran ubicados los equipos de cómputos.
- Se debería establecer un proceso de organización de la información física que se encuentran ubicados en sitio accesible al personal.
- De acuerdo a las observaciones realizadas en la oficina Administrativa, no cuentan con una buena ubicación de los equipos de computo ya que se vuelve un inconveniente para los accesos y salidas de la misma
- Se debe establecer una política de seguridad en el cableado estructurado de la red de las oficinas

Garantizar la seguridad en los sistemas

- Establecer procedimientos para la realización de inventario de aplicaciones el cual como mínimo debe incluir el número de versión instalada, la fecha de instalación, la última fecha de mantenimiento realizado, la plataforma de trabajo, en caso que se adquiera el software se debe registrar el número del documento con el que ingresa, el número de licencia, y el número del manual que se puede consultar para su mantenimiento y utilización. EL inventario de aplicaciones se debe realizar a cada computadora existente en la dependencia de Dirección.

- Realizar mantenimiento preventivo de equipos informáticos para reducir el índice de equipos dañados, minimizar la interrupción en las tareas del usuario con el equipo dañado y evitar el pago a terceros por el soporte técnico.

- Controlar el ingreso de software y aplicaciones en las dependencias por el personal.

- La copia de seguridad debe realizarse semanalmente quedando una copia en la Empresa y la otra debe ser guardada fuera de la Empresa en caso de que sucediera algún desastre.

- Desarrollar y hacer uso de normas y procedimientos para la instalación y la actualización periódica de productos antivirus.

- Implementar procesos de evaluación de los aplicativos que permitan identificar fallas o deficiencias que conlleven a la necesidad de realizar actualizaciones o impliquen el desarrollo de nuevas soluciones o la adquisición de este.

- Desarrollar y documentar planes de contingencia.

- Se debe tener actualizada la base de datos para la liquidación del pago del impuesto con las resoluciones emitidas por el IGAC.

- Se debe corregir los fallos de seguridad en las conexiones simultaneas que se presenta en los usuarios

- La dirección debe aprobar un documento de política de seguridad de la información, publicarlo y comunicarlos a todos los empleados. El documento debe tener estipulado la creación de cuentas de usuario con sus respectivos permisos para impedir el acceso a personal no autorizado y permisos adecuados para su cargo.

- Definir claramente las responsabilidades en cuanto a la seguridad de la información.

- La información se debería clasificar en término de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

- Todos los empleados de la dependencia deberían recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización según sea pertinente para sus funciones laborales.

- Debería existir un proceso disciplinario formal para los que cometan alguna violación de seguridad.

- Restringir la descarga inescrupulosa de programa y su instalación, solo permitir personal autorizado lo haga.

- Se deberían establecer directrices para no permitir comer, beber, fumar en las instalaciones donde se encuentra el servidor encargado del almacenamiento de la información.

- Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

- La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

- La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

- Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

RIESGOS ASOCIADOS																
ID	Nombre del Riesgo	Descripción del riesgo	Posibles consecuencias	Impacto			Probabilidad			Valoración del Riesgo (1 +P)					Manejo del Riesgo	Medidas
				1	2	3	1	2	3	2 Aceptable	3 Tolerable	4 Moderado	5 Importante	6 Inaceptable		
1	Evasión	No efectuar cruces de información en forma oportuna	Disminución del Recaudo			X		X					Importante		Prevenir el riesgo Proteger la Entidad Compartir	Efectuar acuerdos entre los entes que suministran la Información. Realizar censos a las actividades económicas
2	Base de datos desactualizada	No incluir las resoluciones de actualización de predios a la base de datos	Disminución del Recaudo			X	X						Moderado		Asumir, reducir el riesgo	Inclusión oportuna de las resoluciones
3	Desconocimiento de la normatividad vigente	No aplicar las normas relativas al proceso de recaudo	Sanciones Disciplinarias			X		X					Importante		Prevenir el riesgo Proteger la Entidad Compartir	Actualización permanente
4	Desactualización de la información de entes externos	Los entes suministran características de identificación de predios errada	Incumplimiento del debido Proceso. Recuperación Insatisfactoria			X	X						Moderado		Asumir, reducir el riesgo	Verificación y cruce de Información

5	Inundaciones	Ubicación de las instalaciones en sector de alto riesgo	Perdida de documentación de suma importancia para el área			**X**		**X**		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Planes de contingencia causados por desastres climáticos.
6	Incendio	Presencia de material inflamable en el área lo cual puede propiciar un incendio.	Perdida de documentación de suma importancia para el área.			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Equipar el área con extintores de fuegos, colocar señalización de salida de emergencia
7	Virus informáticos	Ausencia de mecanismos de identificación de incidentes o problemas de TI	Rendimiento de los equipos de cómputos muy bajo y ocasionar daño a la información		X				X	Importante	Prevenir el riesgo Proteger la Entidad Compartir	Actualización permanente de los antivirus
8	Fallas del fluido eléctrico	Ausencia de contrato de revisión anual por instalador autorizado	Retraso en las operaciones llevada a cabo en las oficinas de impuesto predial			**X**		**X**		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Mantenimiento preventivo al fluido eléctrico
9	Fraude interno	Perdida derivada de algún tipo de actuación destinada a cometer fraude, o eludir leyes por parte de alguna persona interna de la empresa.	Descuadre de la información recaudada			**X**		X		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Realizar cortes mensuales o bimensualesDel dinero recaudado, asignar funciones y responsabilidades fijas

10	Robo de información	El lugar donde se realiza el trabajo no cuenta con la seguridad necesaria para el tranquilo desenvolvimiento de las actividades Laborales.	Perdida de información vulnerable del área			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Agregar una puerta en la oficina de recaudo pararestringir el paso a personas que no laboran en el área.
11	Daño físicos de discos duros	Perdida de información importante por falta de mantenimiento	Pérdida de información de gran valor del área			**X**		X		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Tener copias de respaldo en caso de daños en el disco
12	Perdida de información	No se cuenta con una organización de la información contenida en el área de impuesto predial	Retraso en la información que se necesite en el momento			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Organizar la documentación en archivadores con seguros, para evitar perdidas
13	Interrupciones organizadas o deliberadas	Que se forma una marcha o protestas por medio de trabajadores públicos	Se deja de recibir ingresos por el tiempo que dure la protesta			**X**		X		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Planes de contingencia
14	Daño a las copias de respaldo	Se debe contar con copias de seguridad	Perdida de datos importantes			**X**	**X**			Moderado	Asumir, reducir el riesgo	Se deben de tener planes de contingencia a la hora que se presente el daño
15	Falta de experiencia del personal	No se cuente con personas, con la experiencia requerida en el cargo	No se lleva acabo las tareas en el tiempo estipulado por la entidad			**X**		X		Importante	Prevenir el riesgo Proteger la Entidad Compartir	Se debe capacitar mas al personal que labora en el área

16	Falta de mantenimiento de los equipos	No se lleve acabo un plan para realizar el mantenimiento debido a los equipos	Retraso en las operaciones que se deben llevar a diario en el área			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Plan de mantenimiento preventivo constante de los equipos de computo
17	Exposición a sustancias nocivas	El área presenta mucho polvo lo cual afecta la salud del empleado	Alergias que pueden contraer los empleados en el área afectada		X			X		Moderado	Asumir, reducir el riesgo	Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente
18	Falla en el sistema contra incendios	No cuentan con planes de contingencia en caso de un incidente	Perdidas económicas o de información en el área			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Se debe contar con extintores y realizarle mantenimiento periódico para prevenir incidentes
19	Falla en la red de datos	No cuentan con un buen diseño y estándar en la red que facilite su optimo trabajo	La información requerida no es obtenida en el tiempo deseado por parte de los funcionarios		X			X		Moderado	Asumir, reducir el riesgo	Utilizar técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.
20	Acceso no autorizado a los datos	Acceso de personal no autorizado a la información almacenada en copias de respaldo	Robo de la información confidencial de las operaciones llevadas a cabo en las oficinas de impuesto predial			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Establecer una política de seguridad. Establecer estándares para la política de seguridad

21	Segregación incorrecta de funciones	Evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a la consumación de un fraude.	Pérdida o modificación de la información por parte del personal que elabora en las dependencias de la secretaría de hacienda.			**X**			X	Inaceptable	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas

MAPA DE RIESGOS

		IMPACTO		
		(1) Ligeramente Dañino	(2) Dañino	(3) Extremadamente Dañino
PROBABILIDAD	(1) Baja			2 – 4 – 14 -
	(2) Media		17 -	1 – 3 – 5 – 8 – 9 – 11 – 13 – 15 -
	(3) Alta		7 -	6 – 10 – 12 – 16 – 18 – 20 - 21

	Inaceptable
	Importante
	Moderado
	Tolerable
	Aceptable

ID	Nombre del Riesgo	Descripción del riesgo	Valoración del Riesgo					Manejo del Riesgo	Medidas	Responsable	Impacto			Probabilidad			Valoración del riesgo después de los controles				
			2 Aceptable	3 Tolerable	4 Moderado	5 Importante	6 Inaceptable				1	2	3	1	2	3	2 Aceptable	3 Tolerable	4 Moderado	5 Importante	6 Inaceptable
6	Incendio	Presencia de material inflamable en el área	INACEPTABLE					Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Equipar el área con extintores de fuegos, colocar señalización de salida de emergencia	Jefe de servicios a operaciones		X		X			TOLERABLE				
10	Robo de información	El lugar donde se realiza el trabajo no cuenta con la seguridad necesaria para el tranquilo desenvolvimiento de las actividades laborales	INACEPTABLE					Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Agregar una puerta en la oficina de recaudo para restringir el paso a personas que no laboran en el área.	Jefe de servicios a operaciones		X		X			TOLERABLE				
12	Perdida de información	No se cuenta con una organización de la información contenida en el área de impuesto predial	INACEPTABLE					Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Organizar la documentación en archivadores con seguros, para evitar perdidas		X			X			ACEPTABLE				

16	Falta de mantenimiento de los equipos	No se lleve acabo un plan para realizar el mantenimiento debido a los equipos	INACEPTABLE	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Plan de mantenimiento preventivo constante de los equipos de computo	Jefe de sistemas		X		X			TOLERABLE
18	Falla en el sistema contra incendios	No cuentan con planes de contingencia en caso de un incidente	INACEPTABLE	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Se debe contar con extintores y realizarle mantenimiento periódico para prevenir incidentes	Jefe de mantenimiento		X		X			TOLERABLE
20	Acceso no autorizado a los datos	Acceso de personal no autorizado a la información almacenada en copias de respaldo	INACEPTABLE	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Establecer una política de seguridad. Establecer estándares para la política de seguridad	Jefe de sistemas	X			X			ACEPTABLE
21	Segregación incorrecta de funciones	Evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a la consumación de un fraude.	INACEPTABLE	Evitar el riesgo Prevenir el riesgo Proteger la Entidad Compartir	Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas	Secretario de Hacienda		X			X		MODERADO
1	Evasión	No efectuar cruces de información en forma oportuna	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Efectuar acuerdos entre los entes que suministran la Información. Realizar censos a las actividades	Secretario de hacienda		X		X			TOLERABLE

					económicas								
3	Desconocimiento de la normatividad vigente	No aplicar las normas relativas al proceso de recaudo	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Actualización permanente	Auxiliar contable	X			X			ACEPTABLE
5	Inundaciones	Ubicación de las instalaciones en sector de alto riesgo	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Planes de contingencia causados por desastres climáticos.	Jefe de servicios a operaciones		X		X			TOLERABLE
7	Virus informáticos	Ausencia de mecanismos de identificación de incidentes o problemas de TI	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Actualización permanente de los antivirus	Jefe de sistemas	X			X			ACEPTABLE
8	Fallas del fluido eléctrico	Ausencia de contrato de revisión anual por instalador autorizado	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Mantenimiento preventivo a las redes eléctricas.	Jefe de mantenimiento		X		X			TOLERABLE
9	Fraude interno	Perdida derivada de algún tipo de actuación destinada a cometer fraude, o eludir leyes por parte de alguna persona	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Realizar cortes mensuales o bimensuales del dinero recaudado, asignar funciones y responsabilidades	Secretario de Hacienda		X		X			TOLERABLE

		interna de la empresa.			fijas								
11	Daño físicos de discos duros	Perdida de información importante por falta de mantenimiento	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Tener copias de respaldo en caso de daños en el disco	Jefe de Sistemas		X			X		MODERADO
13	Interrupciones organizadas o deliberadas	Que se forma una marcha o protestas por medio de trabajadores públicos	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Planes de contingencia	Secretario de Hacienda	X				X		TOLERABLE
15	Falta de experiencia del personal	No se cuente con personas, con la experiencia requerida en el cargo	IMPORTANTE	Prevenir el riesgo Proteger la Entidad Compartir	Se debe capacitar mas al personal que labora en el área	Secretario de hacienda	X			X			ACEPTABLE
2	Base de datos desactualizada	No incluir las resoluciones de actualización de predios a la base de datos	MODERADO	Asumir, reducir el riesgo	Inclusión oportuna de las resoluciones	Administrador de la Base de Datos	X			X			ACEPTABLE
4	Desactualización de la información de entes externos	Los entes suministran características de identificación de predios errada	MODERADO	Asumir, reducir el riesgo	Verificación y cruce de Información	Administrador de la Base de Datos		X		X			TOLERABLE
14	Daño a las copias de respaldo	Se debe contar con copias de seguridad	MODERADO	Asumir, reducir el riesgo	Se deben de tener planes de contingencia a la hora que se presente el	Jefe de sistemas	X			X			ACEPTABLE

					daño								
17	Exposición a sustancias nocivas	El área presenta mucho polvo lo cual afecta la salud del empleado	MODERADO	Asumir, reducir el riesgo	Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente	Jefe de servicios a operaciones		X		X			TOLERABLE
19	Falla en la red de datos	No cuentan con un buen diseño y estándar en la red que facilite su optimo trabajo	MODERADO	Asumir, reducir el riesgo	Utilizar técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.	Administrador de la red		X		X			TOLERABLE

		IMPACTO		
		(1) Ligeramente Dañino	(2) Dañino	(3) Extremadamente Dañino
PROBABILIDAD	(1) Baja	12 – 20 – 3 – 7 – 15 – 2 – 14 -	6 – 10 – 16 - 18 – 1 – 5 – 8 – 9 – 13 – 4 – 17 - 19	
	(2) Media		21 – 11 –	
	(3) Alta			

	Inaceptable
	Importante
	Moderado
	Tolerable
	Aceptable

CONCLUSIÓN

Estar en constantes cambios tecnológicos representa cambios significativos en la toma de decisiones al momento de adquirir infraestructura tecnológica, tratando de proteger, asegurar y minimizar los riesgos que atenten con la información de la empresa, con el fin de mejorar el funcionamiento de la misma, por tal motivo la Secretaria de Hacienda del Municipio de Sabanagrande considere la auditoria de sistemas como una metodología que le permita fortalecer los procesos, basándonos en los más importantes estándares de calidad y seguridad de la información.

Fortalecer los procesos para proteger la información es una prioridad para esta dependencia ya que maneja mucha información confidencial.

En este proyecto se busco implementar una metodología que brindara Confiabilidad, Integridad y Disponibilidad en la infraestructura fisca y tecnológica mejorando el desempeño de los procesos en el información de los datos de una manera segura para los miembros de la secretaría de hacienda del municipio de Sabanagrande.

ISO 27002 y COBIT 4.1 fueron las bases para sustentar las adaptaciones y recomendaciones en busca de mejorar la seguridad de la información, que se ejecutara cuando los diplomáticos lo crean conveniente.

Este proyecto buscó dejar un lineamiento que le permita conocer las mejores prácticas del mercado para soportar la seguridad de su información y la administración de datos y de su ambiente físico.

BIBLIOGRAFIA

Sitio Web: http://moodle.bureauveritasformacion.com/file.php/23/UD01-REVISIoN_NORMA_ISO27001.pdf

Sitio Web: http://www.iso27000.es/iso27000.html#section3

Sitio Web: http://www.monografias.com/trabajos38/cobit/cobit2.shtml

Sitio Web: http://www.marblestation.com/?p=645

COBIT 4.1, ISACA – 2007

ANEXOS

SECRETARIA DE HACIENDA DISTRITAL DEL MUNICIPIO DE SABANAGRANDE

Aplicación De Las Pruebas

1. Prueba de acceso al sistema operativo

Nombre de la prueba	**Objetivo**	**Tipo de prueba**
Prueba de acceso al sistema operativo	Garantizar el ingreso a las cuentas de usuarios del sistema por medio de claves de acceso por parte del personal autorizado	Validación

Descripción
• Observar y confirmar que el sistema al iniciar sesión cuente con clave de acceso • Solicitar a la persona encargada que ingrese al sistema para verificar la seguridad de usuario y clave. • Se observa y se confirma que el equipo no posee clave de acceso al momento de ingresar al sistema

Evidencia	**Resultado**
SHDMS-ASI -01	No satisfactoria.

2. Prueba para validar programas instalados en los equipos de cómputo

Nombre de la prueba	**Objetivo**	**Tipo de prueba**
Prueba para validar programas instalados en los equipos de cómputo	Validar la existencia de programas sumamente perjudiciales instalados en los equipos de computo	Validación
Descripción		
• Se solicita acceso físico en unos de los equipos de cómputo o conexión vía acceso remoto . • Se realiza una búsqueda con el fin de encontrar programas sumamente perjudiciales que no deben estar instalados en los equipos de cómputo. • Confrontar los resultados con el administrador de T.I.		
Evidencia	**Resultado**	
SHDMS-ASI-02	No satisfactoria	

3. Prueba para validar el programa antivirus instalado

Nombre de la prueba	Objetivo	Tipo de prueba
Prueba para validar el programa antivirus instalado	Verificar que el programa antivirus instalado se encuentra protegiendo el sistemas de amenazas	Validación
Descripción		
• Solicitar el ingreso de una memoria USB en uno de los equipo de computo • Verificar si al momento de ingresar la USB el programa antivirus se encuentra protegiendo el sistema. • Se observa y se confirma que el sistema se encuentra desprotegido por el antivirus • Confrontar los resultados con el administrador de T.I.		
Evidencia	**Resultado**	
SHDMS-ASI -03	No satisfactoria	

4. Prueba de verificación de respaldo a los equipos de computo donde se encuentra instalado el aplicativo Transfor

Nombre de la prueba	**Objetivo**	**Tipo de prueba**
Prueba de verificación de respaldo a los equipos de computo donde se encuentra instalado el aplicativo Transfor	Validar la existencia de políticas de respaldo en los equipos de computo donde se encuentra instalado el aplicativo Transfor	Cumplimiento
Descripción		
• Solicitar acceso físico en uno de los equipos donde se encuentra instalado el aplicativo. • Se ejecuta el aplicativo para realizar una copia de seguridad de la información • Al momento de realizar la copia de seguridad el aplicativo no la realiza		
Evidencia	**Resultado**	
SHDMS-ASI-04	No satisfactoria	

5. Prueba de conexiones simultaneas con el mismo usuario

Nombre de la prueba	**Objetivo**	**Tipo de prueba**
Prueba de conexiones simultaneas con el mismo usuario	Verificar que el aplicativo Transfor valide las conexiones activas para no permitir conexiones simultáneas realizadas con un mismo usuario.	Validación

Descripción
• Solicitar un usuario común e ingresar en el aplicativo Transfor. • Ingresar al aplicativo Transfor desde una computadora. • Tratar de Ingresar con el mismo usuario desde otra computadora para confirmar que no valide la conexión existente y no permite el ingreso. • Confrontar el resultado arrojado.

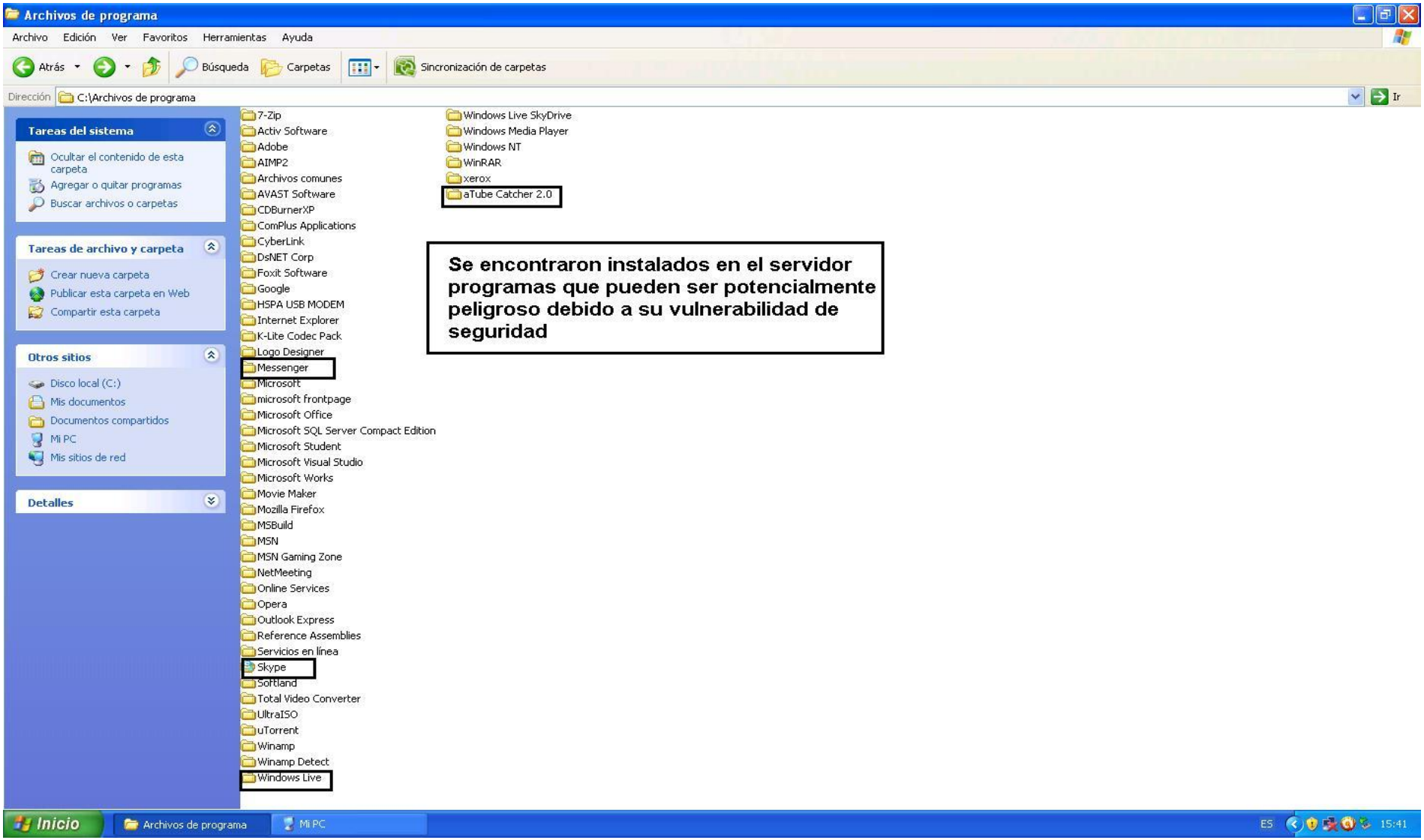
Evidencia	**Resultado**
SHDMS-ASI-05	No satisfactoria

Prueba de acceso al sistema operativo

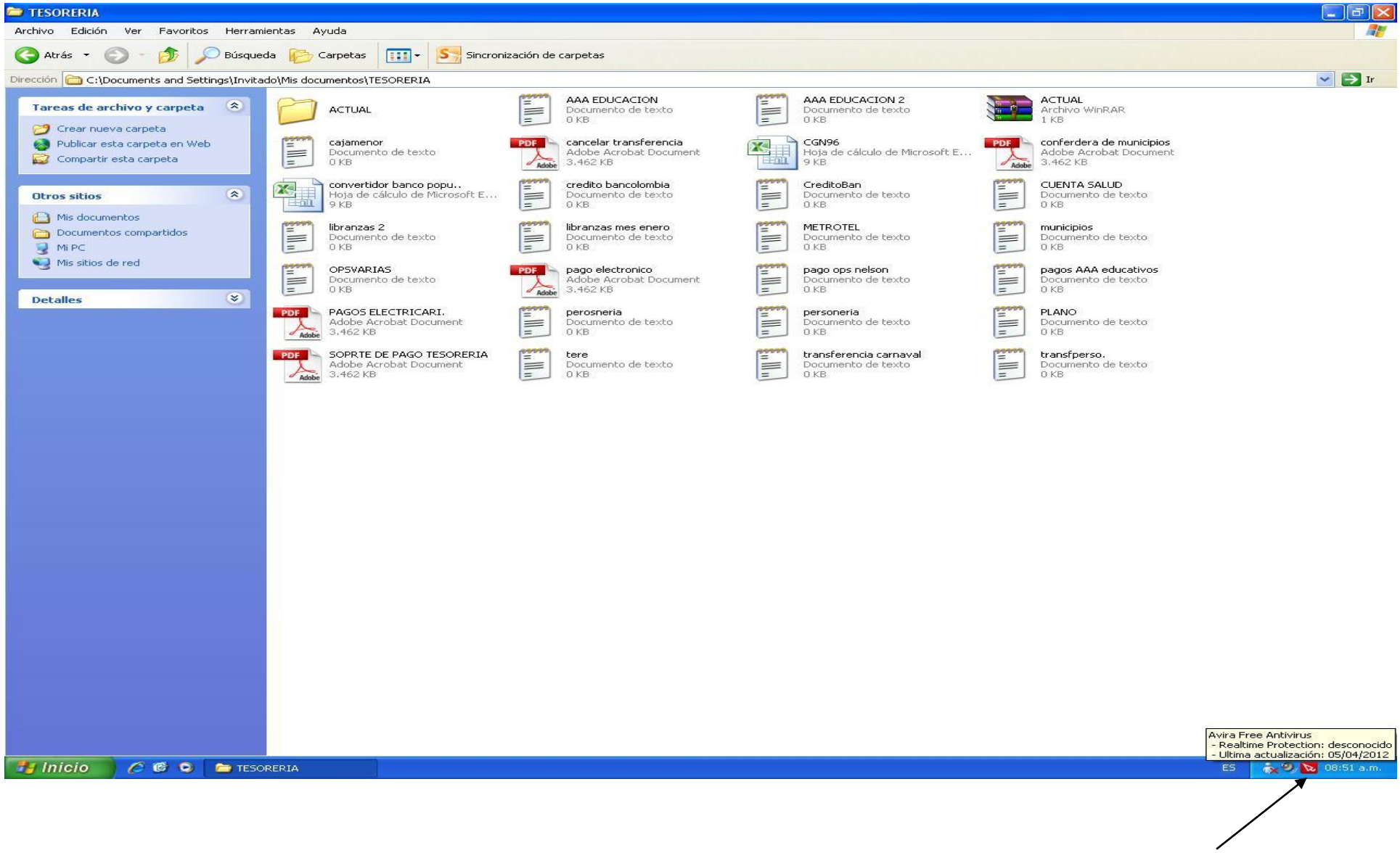
Se procede a ingresar al sistema operativo para validar usuario y contraseña en el equipo de cómputo

Se verifica que el equipo de cómputo no está configurado al inicio de sesión con el usuario y la clave de acceso

Prueba para validar programas instalados en los equipos de cómputo



Prueba para validar el programa antivirus instalado



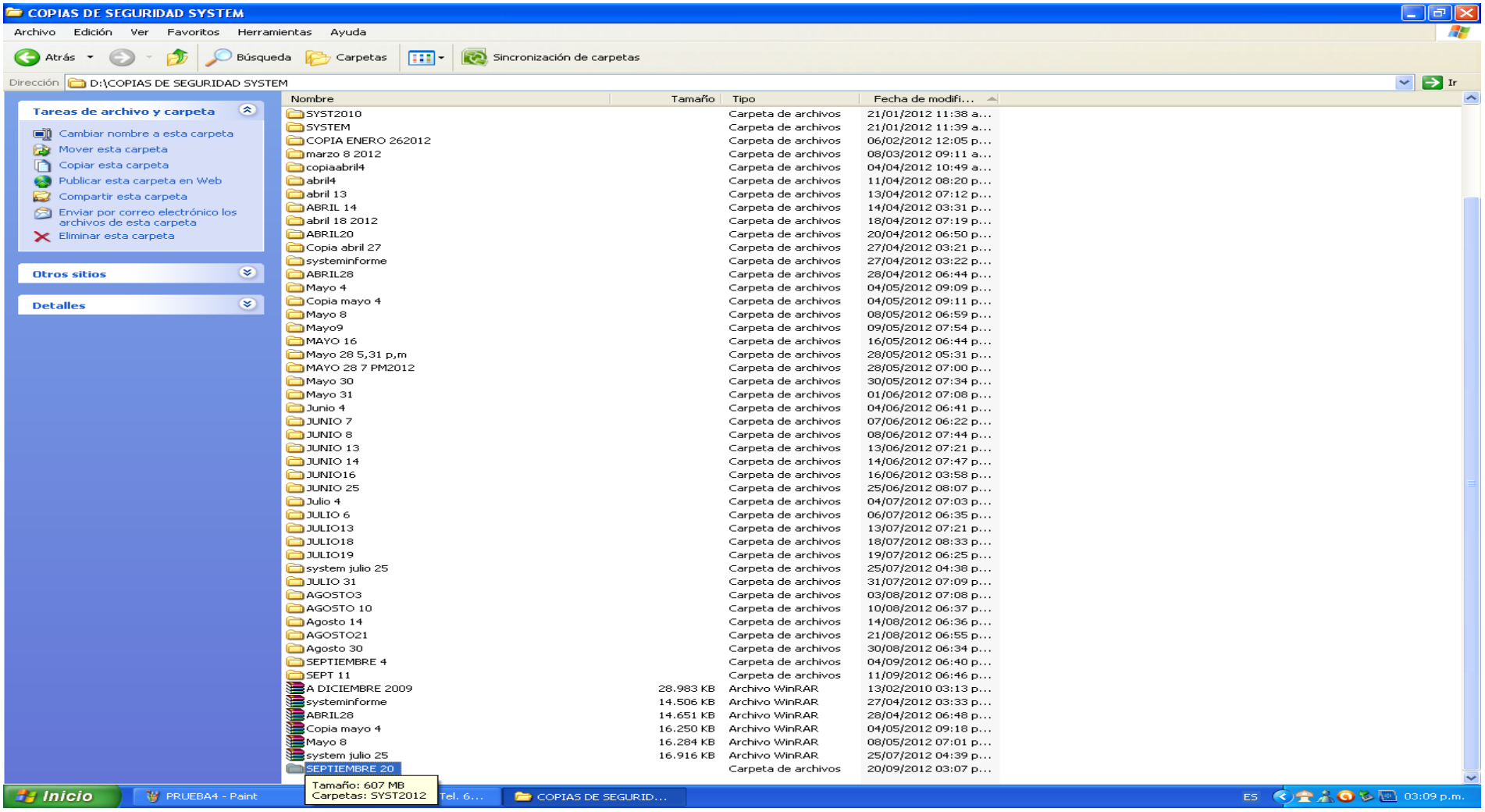
Se comprueba que el programa antivirus ha caducado y hasta la fecha no lo han actualizado

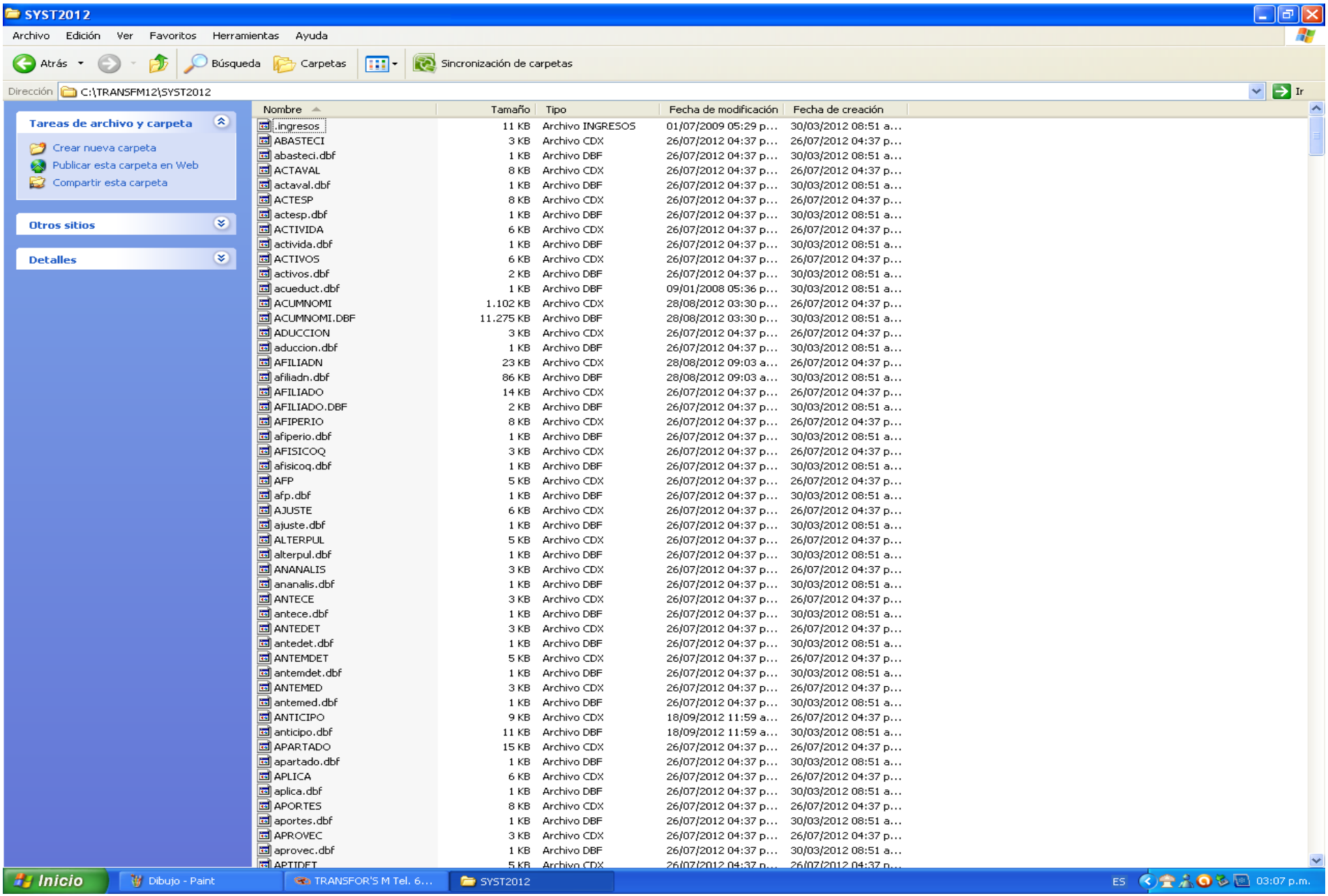
SECRETARIA DE HACIENDA DISTRITAL DEL MUNICIPIO DE SABANAGRANDE

SHDMS-ASI-04

Prueba de verificación de respaldo a los equipos de cómputo donde se encuentra instalado el aplicativo Transfor

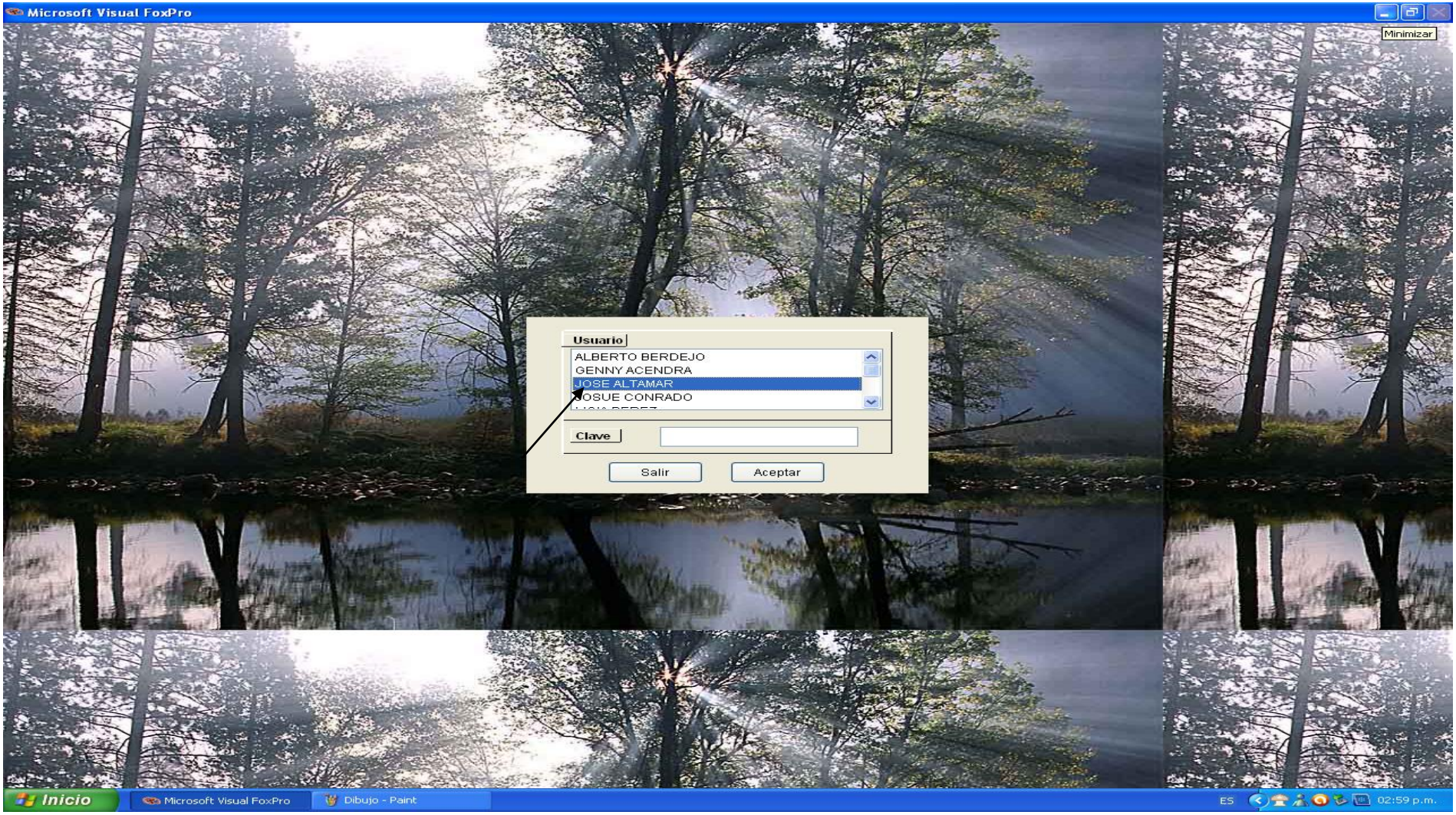
El aplicativo transfor tiene la opción de copias de seguridad pero no funciona y les toca llevarla a cabo manualmente por parte de los empleados

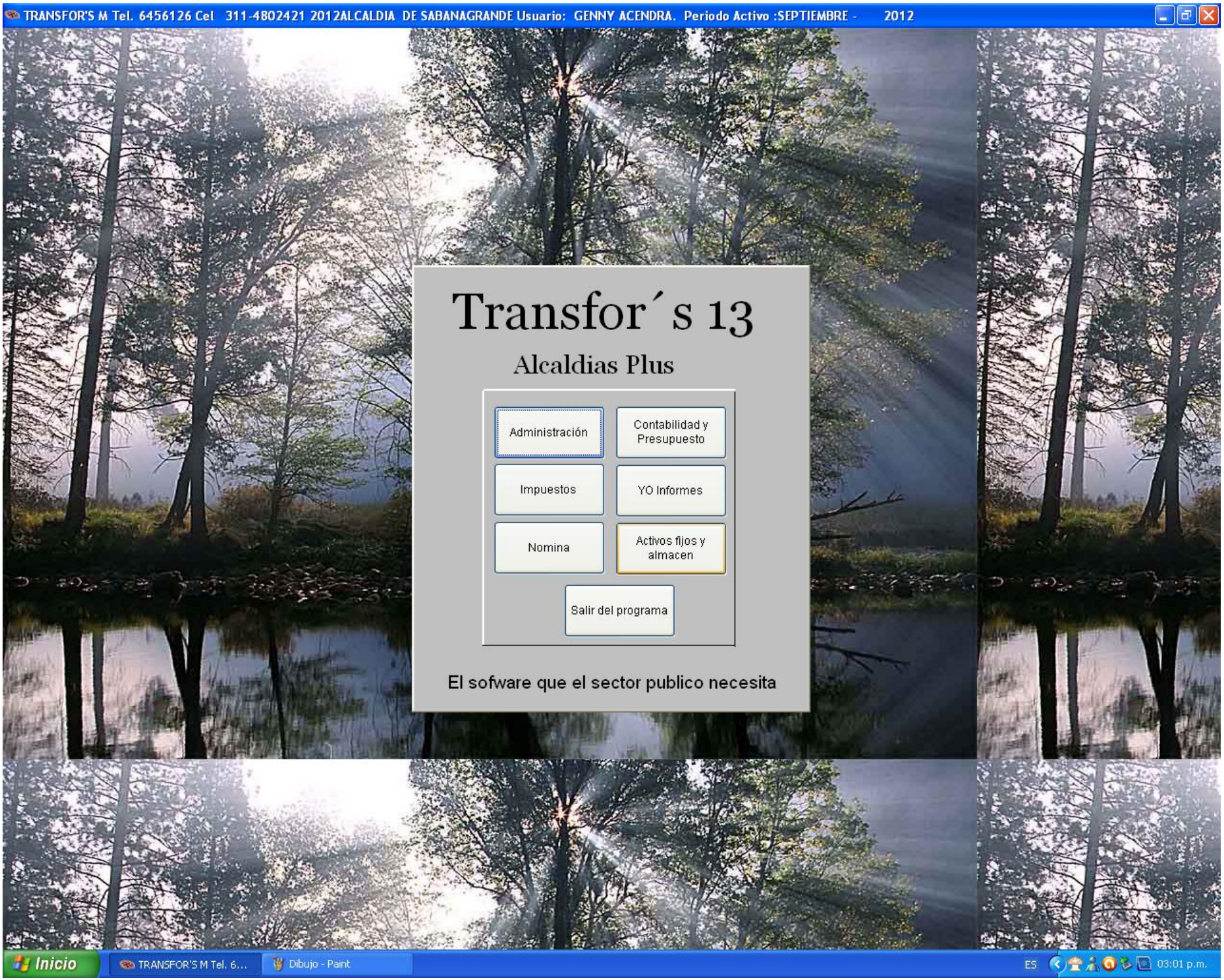



SYST2012
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Carpetas Sincronización de carpetas
Dirección C:\TRANSFM12\SYST2012
Ir
Tareas de archivo y carpeta
Crear nueva carpeta
Publicar esta carpeta en Web
Compartir esta carpeta
Otros sitios
Detalles
Nombre Tamaño Tipo Fecha de modificación Fecha de creación
.ingresos 11 KB Archivo INGRESOS 01/07/2009 05:29 p... 30/03/2012 08:51 a...
ABASTECI 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
abasteci.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ACTAVAL 8 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
actaval.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ACTESP 8 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
actesp.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ACTIVIDA 6 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
actividа.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ACTIVOS 6 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
activos.dbf 2 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
acueduct.dbf 1 KB Archivo DBF 09/01/2008 05:36 p... 30/03/2012 08:51 a...
ACUMNOMI 1.102 KB Archivo CDX 28/08/2012 03:30 p... 26/07/2012 04:37 p...
ACUMNOMI.DBF 11.275 KB Archivo DBF 28/08/2012 03:30 p... 30/03/2012 08:51 a...
ADUCCION 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
aduccion.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
AFILIADN 23 KB Archivo CDX 28/08/2012 09:03 a... 26/07/2012 04:37 p...
afiliadn.dbf 86 KB Archivo DBF 28/08/2012 09:03 a... 30/03/2012 08:51 a...
AFILIADO 14 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
AFILIADO.DBF 2 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
AFIPERIO 8 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
afiperio.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
AFISICOQ 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
afisicoq.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
AFP 5 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
afp.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
AJUSTE 6 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
ajuste.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ALTERPUL 5 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
alterpul.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANANALIS 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
ananalis.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANTECE 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
antece.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANTEDET 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
antedet.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANTEMDET 5 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
antemdet.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANTEMED 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
antemed.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
ANTICIPO 9 KB Archivo CDX 18/09/2012 11:59 a... 26/07/2012 04:37 p...
anticipo.dbf 11 KB Archivo DBF 18/09/2012 11:59 a... 30/03/2012 08:51 a...
APARTADO 15 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
apartado.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
APLICA 6 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
aplica.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
APORTES 8 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
aportes.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
APROVEC 3 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
aprovec.dbf 1 KB Archivo DBF 26/07/2012 04:37 p... 30/03/2012 08:51 a...
APTIDET 5 KB Archivo CDX 26/07/2012 04:37 p... 26/07/2012 04:37 p...
Inicio
Dibujo - Paint
TRANSFOR'S M Tel. 6...
SYST2012
ES
03:07 p.m.

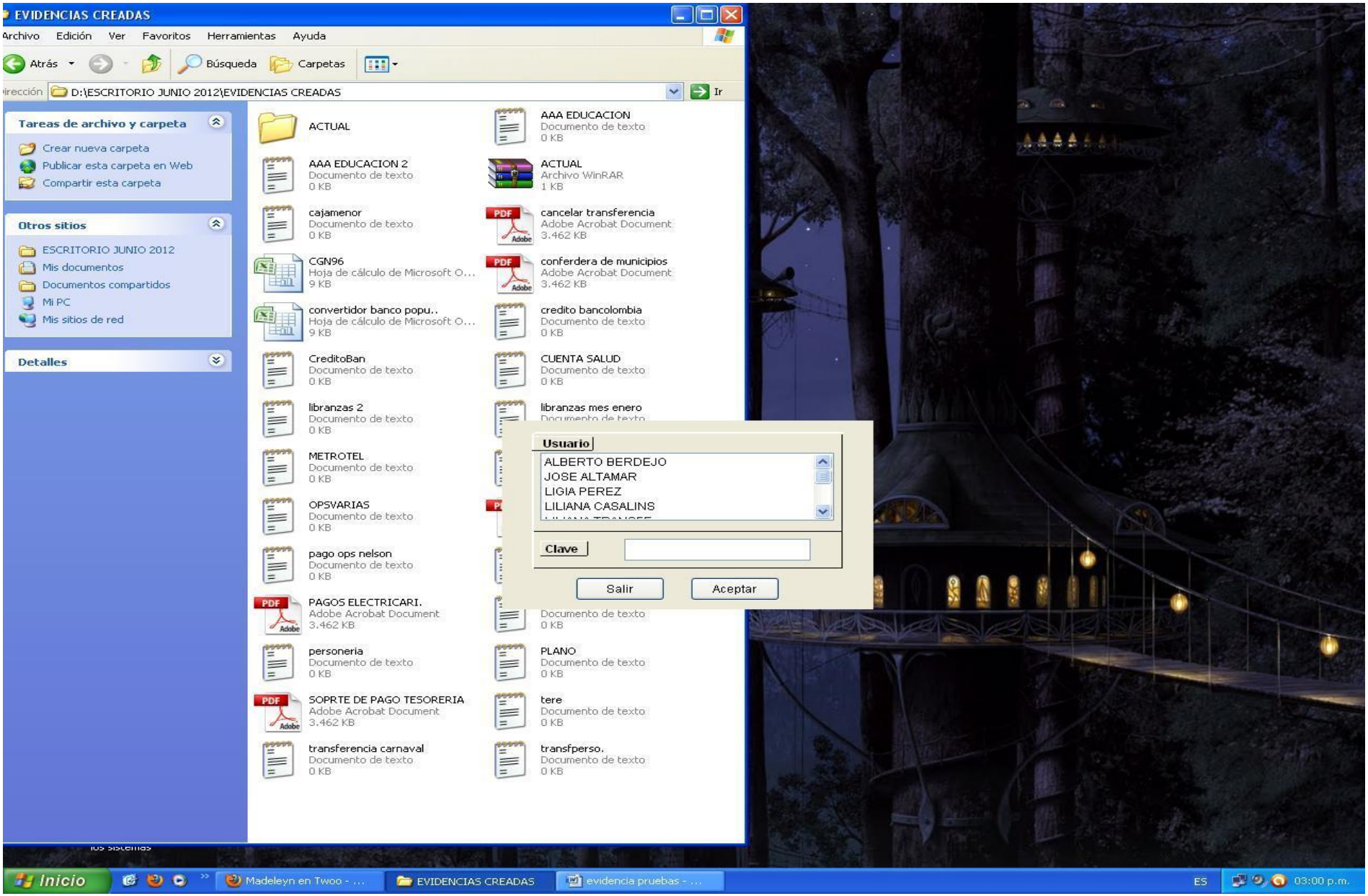
Prueba de conexiones simultaneas con el mismo usuario

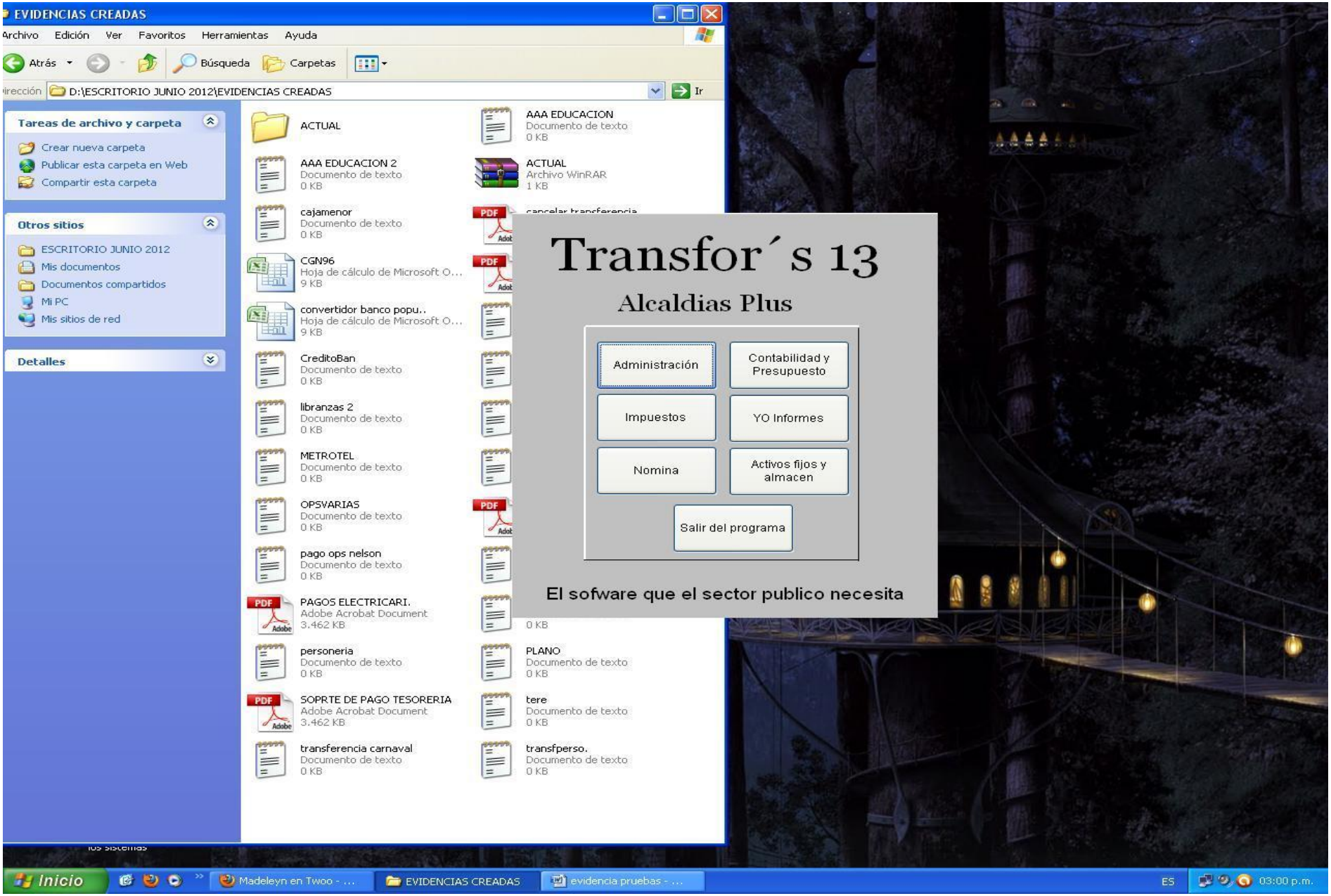
Acceso con el usuario de prueba **José Altamar** en el equipo 1




TRANSFOR'S M Tel. 6456126 Cel 311-4802421 2012ALCALDIA DE SABANAGRANDE Usuario: GENNY ACENDRA. Periodo Activo :SEPTIEMBRE - 2012
Transfor´s 13
Alcaldias Plus
Administración
Contabilidad y Presupuesto
Impuestos
YO Informes
Nomina
Activos fijos y almacen
Salir del programa
El sofware que el sector publico necesita
Inicio
TRANSFOR'S M Tel. 6...
Dibujo - Paint
ES
03:01 p.m.

Con el mismo usuario **José Altamar** se accede simultáneamente desde otro equipo, permitiendo el acceso




EVIDENCIAS CREADAS
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Carpetas
D:\ESCRITORIO JUNIO 2012\EVIDENCIAS CREADAS
Tareas de archivo y carpeta
Crear nueva carpeta
Publicar esta carpeta en Web
Compartir esta carpeta
Otros sitios
ESCRITORIO JUNIO 2012
Mis documentos
Documentos compartidos
Mi PC
Mis sitios de red
Detalles
ACTUAL
AAA EDUCACION 2
Documento de texto
0 KB
cajamenor
CGN96
Hoja de cálculo de Microsoft O...
9 KB
convertidor banco popu..
CreditoBan
libranzas 2
METROTEL
OPSVARIAS
pago ops nelson
PAGOS ELECTRICARI.
Adobe Acrobat Document
3.462 KB
personeria
SOPRTE DE PAGO TESORERIA
transferencia carnaval
AAA EDUCACION
ACTUAL
Archivo WinRAR
1 KB
PLANO
tere
transfperso.
Transfor´s 13
Alcaldias Plus
Administración
Contabilidad y Presupuesto
Impuestos
YO Informes
Nomina
Activos fijos y almacen
Salir del programa
El sofware que el sector publico necesita
Inicio
Madeleyn en Twoo - ...
EVIDENCIAS CREADAS
evidencia pruebas - ...
ES
03:00 p.m.

LISTA DE CHEQUEO

Item	Requerimiento	Cumple		
		SI	NO	N/A
1	El aplicativo genera reportes propios del áreas de negocio			
2	El aplicativo genera reportes para otras áreas del negocio			
3	Existe otra persona diferente al administrador o funcional con conocimientos funcionales del aplicativo Transfor			
4	Existe más de un usuario con rol de administrados en custodia			
5	Existe la figura de usuario administrador en custodia			
6	Manejan reportes de usuarios con acceso a la aplicación y a la base de datos.			
7	Existe matriz de roles y perfiles activos definidas para la aplicación Transfor			
8	Validan los usuarios y perfiles activos en la aplicación Transfor			
9	Las cuentas de usuarios que han sido dados de baja en la empresa o que están de licencias o de vacaciones se encuentran activas			
10	Existen políticas de respaldos para la aplicación			
11	Existen procedimientos de revisiones periódicos de backups para la aplicación Transfor			
12	Existen procedimientos de backups			
13	Cuentan manuales de usuarios para la aplicación Transfor			
14	Disponen de ambiente de certificación independiente al ambiente de Producción			
15	Cuentan con bitácora de fallas			

16	Existen manuales técnicos de la aplicación Transfor			
17	Existe esquema de la infraestructura tecnológica			
18	Manejan contingencia para el aplicativo Transfor			
19	Existe documentación de las pruebas realizadas al aplicativo Transfor			
20	Existen minutogramas (Documentos requeridos a la hora de ejecutar una contingencia de una aplicación, define las acciones, tiempos y responsables de la ejecución de cada actividad)			
21	Existen registros de logs de la plicación Transfor			
22	El aplicativo Transfor ha sido inestable en los últimos periodos			
23	Cuentan con indicadores que midan el cumplimiento del proceso para la disponibilidad del aplicativo			
24	La aplicación Transfor realiza correctamente el proceso de carga de la información (en la BD se refleja lo digitado en el sistema).			
25	Diariamente se realiza proceso de cargue de la información generada por las diferentes oficinas de la empresa			
26	Existe manipulación de la información una vez cargada a la base de datos			
27	Existe en la oficina principal soporte físico de la información cargada en la Base de datos y donde reposa			
28	Los DBA tienen acceso a ver toda la información de la base de datos			
29	Mantienen registros de los logs de las acciones ejecutadas en la base de datos			
30	Existe alguien en la compañía que controle las labores administrativas de los DBA			
31	Existe una adecuada ubicación de los servidores y equipos de comunicación (agua, calor, tropiezo)			
32	Obsolescencia en los equipos de cómputo que interactúan con la aplicación Transfor			

33	Espacio suficiente en los discos de almacenamiento			
34	Existencia de Antivirus actualizado en los equipos de cómputo.			
35	Existe control sobre los accesos remotos al servidor			
35	Existe control sobre las carpetas compartidas en el servidor			
36	Todas las aplicaciones que se instalan en el servidor se encuentran certificadas			
37	Los equipos de cómputo tienen aplicaciones no certificadas			
38	Espacio suficiente en los discos de almacenamiento			
39	Existencia de Antivirus actualizado en los equipos de cómputo.			
40	El software Transfor se encuntra debidamente licenciado			
41	Los sistemas operativos de las máquinas de cómputo tienen los parches actualizados			
42	El sistema operativo del servidor tiene los parches de actualización			
43	Existe bitácopa de control de cambios sobre parches y actualizaciones del sistema Opertaivo del servidor			
44	Existe bitácopa de control de cambios sobre parches y actualizaciones de las máquinas de cómputo			
45	El aplicativo Transfor cumple con las necesidades requeridas por la empresa			
46	El aplicativo Transfor maneja los roles definidos			
47	Los roles asignados a los usuarios de Transfor están acorde al perfil y funciones que tienen dentro de la empresa.			
48	Existe procesos para la puesta en producción de nuevos ejecutables de la aplicación			
49	El paso a producción de nuevos ejecutables de la palicación se da en horarios o días no laborales para los usuarios			

50	Los usuarios del sistema han recibido capacitación del mismo			
51	El administrador ha recibido capacitación del sistema Transfor			
52	El sistema Transfor maneja alertas de usuarios			
53	Existe personal que monitoree las alertas del sistema			
54	Existe personal que monitoree los logs del sistema o de la base de datos.			
55	Existe manual de Instalación del aplicativo Transfor			
56	Existe bitácoras de las fallas que ha sufrido el aplicativo			
57	La parametrización del sistema puede hacerse a través del sistema			
58	Las claves de acceso al sistema se encuentran encriptadas en la base de datos			
59	Existe un estándar definido para la creación de usuarios en el sistema			
60	El sistema solicita cambios periódicos de contraseña, de ser así cada cuanto tiempo solicita cambio de contraseña			
61	Pueden estar conectados el mismo usuario en dos máquinas al mismo tiempo			
62	Un usuario desde el sistema puede actualizar la información registrada			
63	Existe personal que monitoree las alertas del sistema			
64	Los campos Críticos en el sistema son de obligatoriedad en la captura de la información			
65	Los usuarios tienen acceso al modulo de reportes del sistema			
66	Existe una figura o rol dentro de la empresa que verifique que la información reportada es real			
67	Existen politicas para el uso de los recursos tecnólogicos			

68	Existe evidencia sobre el cumplimiento de las políticas de seguridad de los recursos tecnológicos			
69	Existen mecanismos de control o de verificación para el cumplimiento de las políticas de seguridad de los equipos suministrados de cómputo			
70	Existe una auditoria anterios de Transfor			
71	Los campos Críticos en el sistema son de obligatoriedad en la captura de la información			
72	El sistema Transfor tiene la opción de guardar reportes			
73	El sistema Transfor tiene la opción para imprimir reportes			
74	Existen procedimientos de emergencia para los recursos informáticos de la empresa			
75	Existe inventario de la infraestructura tecnológica			
76	Se lleva a cabo un programa de mantenimiento preventivo para todos los equipos de la infraestructura tecnológica			
77	Se lleva a cabo un programa de mantenimiento correctivo para todos los equipos de la infraestructura tecnológica			
78	Existe una bitácora sobre el mantenimiento correctivo que se les hace a los equipos de la infraestructura tecnológica			
79	Existe una mesa de ayuda para requerimientos de usuarios internos			
80	Existen controles de acceso al cuarto de servidores			
81	El sistema Transfor tiene la opción de guardar reportes			
82	El sistema Transfor tiene la opción para imprimir reportes			
83	Existen procedimientos de emergencia para los recursos informáticos de la empresa			

84	Existe inventario de la infraestructura tecnológica			
85	Se lleva a cabo un programa de mantenimiento preventivo para todos los equipos de la infraestructura tecnológica			