CONTRALORÍA Municipal de Bucaramanga

INFORME FINAL

AUDITORÍA ESPECIAL EN SEGURIDAD DE LA INFORMACION

CONTRALORA MUNICIPAL DE BUCARAMANGA
Dra. MAGDA MILENA AMADO GAONA

SUBCONTRALOR
Dr. JORGE ELIECER GOMEZ TOLOZA

COORDINADOR DE VIGILANCIA FISCAL Y AMBIENTAL
Dr. JUAN CARLOS NIÑO REY

AUDITORES:

JAIRO RINCON GARCIA
Auditor Fiscal (Líder)

ELKIN ANDRES MOLANO BARREIRO
Contratista de apoyo

CONTRALORÍA
MunicipaldeBucaramanga

TABLA DE CONTENIDO

CONTRALORÍA MunicipaldeBucaramanga

1. HECHOS RELEVANTES EN EL PERIODO AUDITADO

1.1. ALCANCE DE LA AUDITORIA

La Contraloría Municipal de Bucaramanga, en desarrollo de su función constitucional y legal, con fundamento en el Plan General de Auditorías programado y en cumplimiento a la resolución 000236 del 30 de diciembre de 2011, la cual fue modificada por la resolución 000097 del 29 de febrero de 2012 proferida por la Contralora Municipal de Bucaramanga, se practicó Auditoría Especial en Seguridad de la Información.

La auditoria se baso en los controles establecidos en la norma (NTC:ISO/IEC 27001:2005) y se realizó un trabajo metodológico con el fin de identificar debilidades que pudieran comprometer la confidencialidad, disponibilidad e integridad de los datos.

1.2. OBJETIVO GENERAL

Evaluar la gestión y controles realizados según los lineamientos de seguridad de la información enfocados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información según la norma (NTC:ISO/IEC 27001:2005).

1.3 OBJETIVOS ESPECIFICOS

- Identificar los controles que se deberían estar aplicando para garantizar la confidencialidad, integridad y disponibilidad de los activos de información.
- Determinar el estado actual del sistema de gestión de seguridad de la información.
- Identificar los riesgos a los que se encuentra expuestos los activos de información según los dominios, objetivos de control y controles establecidos en la norma (NTC:ISO/IEC 27001:2005).

2. DESARROLLO DE LA AUDITORIA

2.1. Revisión de Conceptos:

- ✓ **Norma (NTC:ISO/IEC 27001:2005):** La norma que en siglas significa Technology Security techniques viene a ser la evolución del estándar de buenas practicas ISO creado en 1995. Este tipo de certificación busca garantizar por medio de controles que los activos de información de la entidad mantengan la confidencialidad, disponibilidad e integridad de los datos.

- ✓ **Funcionamiento de la Norma (NTC:ISO/IEC 27001:2005):** La aplicación de buenas practicas en seguridad de la información sirve para brindar soporte de los datos que se encuentran registrados en la Entidad. Para ello se implementan los controles necesarios para el cuidado de la información brindando confidencialidad, disponibilidad e integridad de los datos para el buen uso de la información y no divulgación de la misma.

- ✓ **Confidencialidad de los datos:** Es cuando un usuario o funcionario de la Entidad garantiza seguridad al momento de ingresar a la información, no divulgando dicha

información a personas ajenas a la Entidad; con ello se busca conseguir que la información sea accedida única y exclusivamente por quien la necesite y este autorizado para utilizarla.

- ✓ **Disponibilidad de los datos:** Es poder acceder a la información de la Entidad en el tiempo o la hora en que sea necesario crear, modificar o respaldar los datos.

- ✓ **Integridad de los datos:** Es poder garantizar que los datos no puedan ser alterados por personas no autorizadas.

- ✓ **Activos de Información:** Son los bienes de la Entidad que se encuentran relacionados de manera directa o indirecta con la actividad, entre los cuales se encuentran:
  - o Medios de comunicación que se utilizan para la transmisión de datos, tales como: redes, correo electrónico, etc.
  - o Medios magnéticos y ópticos de almacenamiento de información como: cintas, discos, memorias, etc.
  - o Programas y aplicaciones de la Entidad, ya sean desarrollos propios o adquiridos por terceros.
  - o Manuales, procedimientos y reglamentaciones afines al área informática.

- ✓ **Vulnerabilidad:** Son errores que permiten realizar acciones desde afuera, sin permiso del administrador del equipo, incluso se puede suplantar a un usuario en común.

- ✓ **Seguridad Informática:** Garantizar que la información privada de la Entidad, sea física o magnética este solo al alcance de las personas con suficientes privilegios para realizar acciones que se les ha otorgado mediante políticas dadas.

- ✓ **Seguridad física:** Por medio de esta seguridad se evita el acceso no autorizado, daños o intromisiones en las instalaciones y a la información de la Entidad; ya que los servicios de procesamientos de información deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados.

- ✓ **Seguridad en las estaciones de trabajo:** Una estación de trabajo es un PC y por tanto toda la información que se produce en la Entidad es importante y normalmente producida en dichas estaciones.

- ✓ **Copias de seguridad:** Todo tipo de respaldo que se realiza con el fin de desempeñar una breve recuperación de los datos y restaurar el original después de perdidas parciales o totales de información importante en la Entidad.

- ✓ **Virus informáticos:** Programas de software que se ejecutan y se propagan localmente, realizando copias de si mismo en otro programa o documento, infectando otros ordenadores. El daño puede ir desde perdida de rendimiento del equipo de computo hasta vulnerabilidad y perdida de información importante.

- ✓ **Código móvil:** código trasferido desde un computador a otro.

2.2. Debilidades encontradas

Acuerdos de Confidencialidad

Se pudo evidenciar que los funcionarios tienen un manual de funciones que habla del tema del control de forma muy generalizada. Por otra parte revisadas algunas minutas de contrato se observa que en la clausula de obligaciones del contratista, se manifiesta la importancia de salvaguardar y manejar con confidencialidad la información bajo responsabilidad y producto del objeto contractual.

Revisión Independiente de la Seguridad de la Información

Actualmente no se ha realizado auditoria alguna relacionada a la seguridad de la información. Aunque se tiene previsto la realización de una auditoria al sistema de información de contabilidad y presupuesto (GD), es importante tener en cuenta que al tema relacionado a los activos de información se le debe prestar más atención por parte de la entidad en relación a la importancia y repercusiones que se puedan generar por el uso no autorizado.

Acuerdos sobre el uso adecuado de los activos de información.

La entidad actualmente no cuenta con un procedimiento formal para funcionarios y contratistas que tienen acceso a los activos de información, donde se especifique la manera adecuada y tratamiento según la importancia de la información para el uso no autorizado de la misma.

Formación y capacitación en seguridad de la información

Aunque se hayan realizado capacitaciones en temas relacionados a conocimientos informáticos y uso adecuado de los equipos de computo, es importante fortalecer a funcionarios y contratistas que tienen acceso a la información sobre los métodos y controles que deben aplicar constantemente para minimizar el riesgo de uso no autorizado.

Cancelación de permisos de acceso

Actualmente la entidad no cuenta con un procedimiento formal para que una vez un funcionario o contratista termine sus labores en forma definitiva en la entidad, inmediatamente le sea restringido el acceso a equipos y sistemas de información.

Perímetro de seguridad física

La entidad se encuentra ubicada dentro de un edificio que ofrece un primer filtro para el ingreso, con sus respectivas cámaras de seguridad ubicadas justamente en la parte exterior de acceso a la entidad.

Controles físicos de entrada

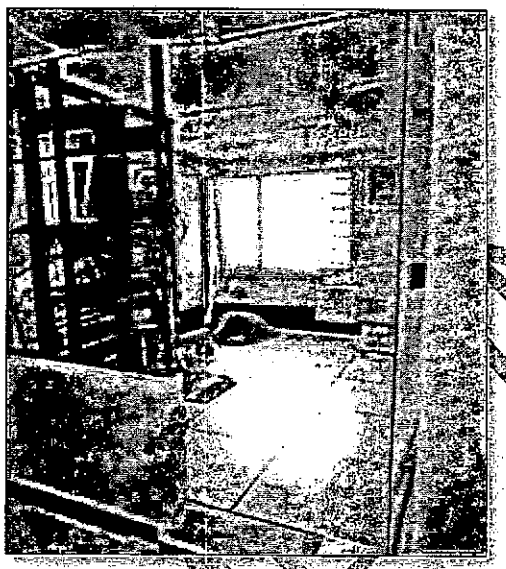
Si bien es cierto que existe un filtro proporcionado por el edificio donde se encuentra ubicada la entidad, es importante resaltar que no existe un control adecuado que garantice que las personas que ingresan hacen parte de la entidad o en su defecto van con el objetivo de adelantar alguna diligencia en la misma.

Seguridad de oficinas y despachos para salvaguardar los activos de información

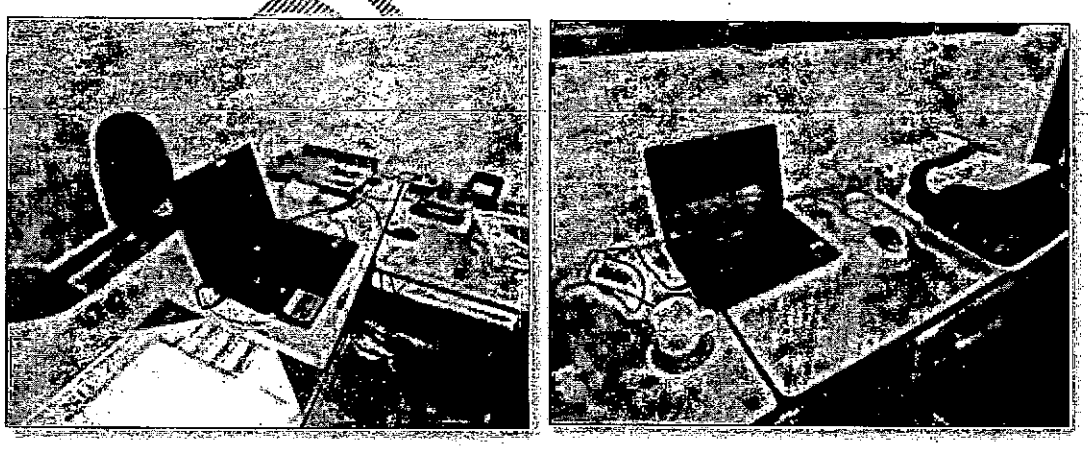
Se pudo evidenciar que la mayoría de las oficinas aunque cuentan con sus respectivos archivadores con seguridad no se están utilizando de la manera correcta, puesto que las llaves son dejadas en el mismo archivador, no ofreciendo ninguna garantía y funcionalidad. Además se observo que si por algún motivo se perdiera algún activo de información no existe la forma en el interior para saber quien pudo obtener dicho activo.

Instalación y protección de equipos

Unos de los factores más importantes en la seguridad de la información esta contemplada en los servidores donde reposan los sistemas de información. Se pudo evidenciar que se cuenta con una restricción para acceder a dicho recurso pero no se esta utilizando, siendo esto una vulnerabilidad con repercusiones negativas para la entidad.



Por otra parte los equipos portátiles donde se procesan los activos de información no cuentan con la suficiente seguridad física que garantice que en algún momento puedan ser extraviados.



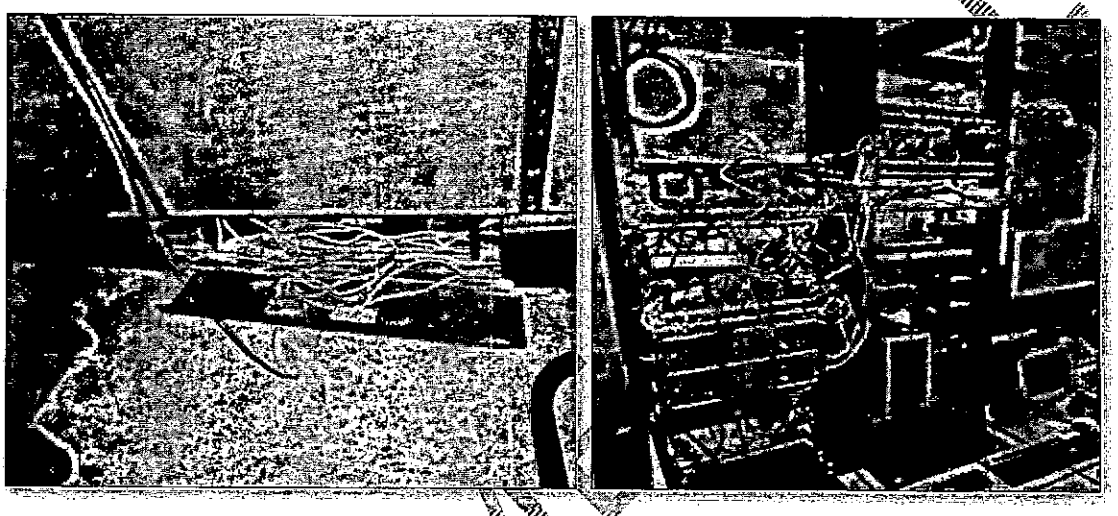
Suministro eléctrico

Actualmente no se cuenta con el suministro eléctrico o control adecuado que garantice la seguridad de los equipos en el momento de una falla eléctrica. Esto es algo muy importante a

tener en cuenta siendo los equipos de cómputo la fuente primaria de creación y modificación de información.

Seguridad del cableado

La entidad cuenta actualmente con su cableado estructurado. Pero se pudo evidenciar que dicho cableado se encuentra expuesto en algunos sectores aumentando los riesgos de fallas en la trasmisión de datos y fallas eléctricas que pudieran repercutir negativamente en la entidad.



Traslado de activos

No se cuenta con un documento formal que garantice el procedimiento adecuado para la reutilización o eliminación (baja) de equipos. Al no contar con dicho procedimiento, se aumenta el riesgo de uso no autorizado de información.

Control de cambios operacionales

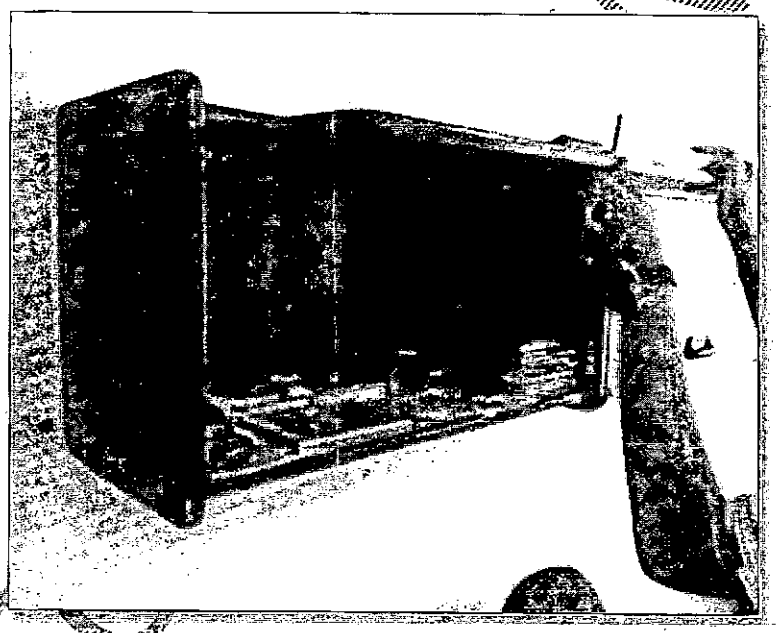
Para poder controlar los cambios en los equipos se crearon perfiles de administrador y limitados en el sistema operativo, pero se pudo evidenciar que algunos equipos no cuentan con los perfiles anteriormente nombrados. Para garantizar que no existan vulnerabilidades todos los equipos deben tener debidamente creados estos perfiles.

Medidas y controles contra código móvil

Actualmente no se cuenta con algún control que garantice la descarga de archivos o software no autorizado. Esto aumenta el riesgo del ingreso de software malintencionado al equipo que pueda afectar la confidencialidad de la información.

Recuperación de la información

Se están realizando copias de seguridad al sistema de información contable (GD), pero es importante que dichas copias o en su defecto la redundancia se encuentren en un lugar que garantice la debida salvaguarda física del disco, dvd o cd. Por otra parte no se observó algún método o herramienta que facilite la realización de copias de seguridad de cada equipo de la entidad.



Gestión de soportes extraíbles

No se cuenta con algún método o herramienta tecnológica que evite la extracción de información por medio de discos o memorias USB a personas no autorizadas. Siendo esto uno de los factores de mayor vulnerabilidad relacionados a la seguridad de la información.

Gestión de contraseñas de usuario

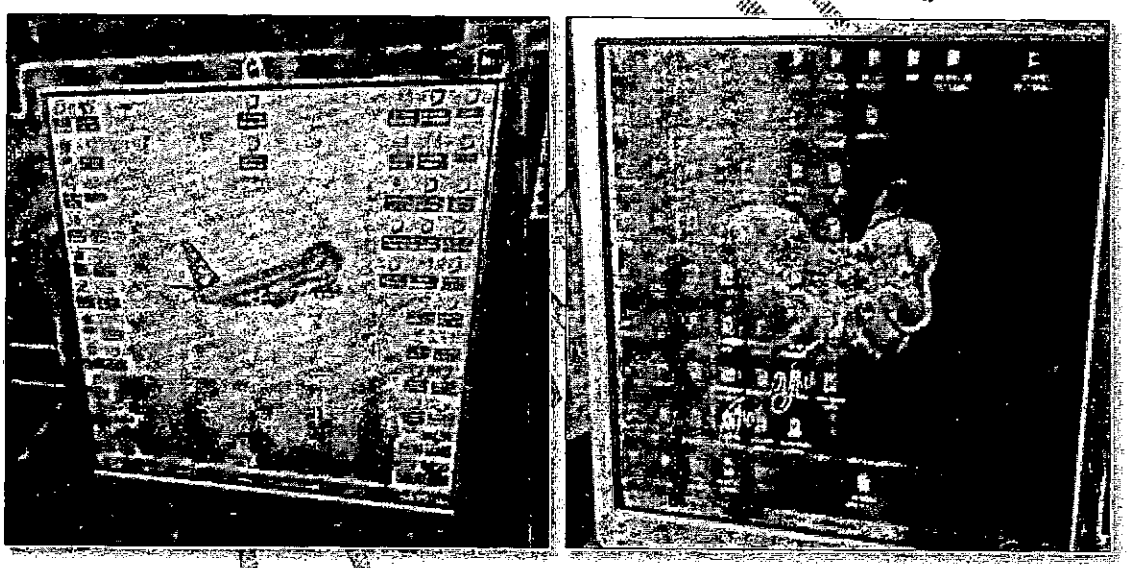
Es importante que los funcionarios o contratistas que tienen acceso a los equipos de cómputo entiendan la importancia de tener y cambiar periódicamente la contraseña de acceso al equipo. A su vez también se debe garantizar que exista un método para recuperar o en su defecto quitar la contraseña creada por personal autorizado.

Revisión de los derechos de acceso de los usuarios

Hasta el momento no se ha solicitado por parte de las directivas listado de usuarios activos en los sistemas de información. Esto es importante ya que demuestra el compromiso de la dirección por mantener un control sobre funcionarios y contratistas con acceso a información tan importante como la contable.

Políticas para escritorios y monitores sin información

Se evidencio que existen en su mayoría archivos ubicados en el escritorio del equipo de cómputo aumentando relevantemente el riesgo de extracción de información a personas no autorizadas.



Autenticación de usuario para conexiones externas

El soporte técnico realizado por el contratista del software contable (GD) es en gran parte por acceso remoto. Es vital que los usuarios que reciben dicho soporte por este medio, entiendan el funcionamiento de la herramienta que utiliza el contratista para acceder al equipo y así minimizar el riesgo de fuga de información.

Sistema de gestión de contraseñas

No se cuenta con un método o herramienta tecnológica que garantice la creación de contraseñas seguras, por lo que existe el riesgo de vulnerar dichas contraseñas y así tener acceso a información importante y privada para la entidad.

Comunicación de debilidades en seguridad

Todos los usuarios deben entender que las debilidades en la seguridad de la información pueden afectar a toda la entidad y por tanto debería informarlas. Actualmente no se pudo evidenciar algún documento o herramienta que facilite a funcionarios o contratistas el conocimiento de vulnerabilidades comunes que pudieran presentarse para informar.

Salvaguarda de los registros de la Organización

Se observo que si algún documento radicado se perdiera, no existe la forma para recuperarlo rápidamente o en su defecto tener acceso a dicho documento dependería de factores externos que la entidad no puede garantizar su efectividad.

En relación al archivo central se esta realizando un proceso de organización física pero falta algún método o herramienta que garantice la integridad de la información al momento de realizar algún préstamo solicitado, puesto que no basta con llevar un control de prestamos o inventario documental sino también poder garantizar que el documento no pueda ser alterado o en consecuencia se pueda recuperar algún folio extraído premeditadamente.

CONTRALORÍA
MunicipaldeBucaramanga

3. CARTA CONCLUSIONES

Bucaramanga, Junio 19 de 2013

Doctora
SILVIA JOHANA CAMARGO GUTIERREZ
Directora
INVISBU
Ciudad

La Contraloría Municipal de Bucaramanga, con fundamento en las facultades otorgadas por los artículos 267 y 272 de la Constitución Política, practicó Auditoria Especial a la Seguridad de la Información.

La auditoria se centro en los controles establecidos en la norma (NTC:ISO/IEC 27001:2005) y se realizó un trabajo metodológico con el fin de identificar debilidades que pudieran comprometer la confidencialidad, disponibilidad e integridad de los datos.

Es responsabilidad del Instituto de Vivienda e Interés Social de Bucaramanga (INVISBU) la información suministrada y analizada por la Contraloría Municipal de Bucaramanga. La responsabilidad de la Contraloría Municipal de Bucaramanga consiste en producir un informe integral que contenga las conclusiones relacionadas a debilidades encontradas sobre seguridad de la información; así como las políticas y los procedimientos de auditoría establecidos por la Contraloría Municipal de Bucaramanga, por tanto, requirió acorde con ellas, la planeación y ejecución del trabajo, de manera que la auditoría proporcione una base razonable para fundamentar las conclusiones expresadas en el informe.

CONCLUSIONES

Teniendo en cuenta la importancia que representa los activos de información en la entidad y poder garantizar la confidencialidad, disponibilidad e integridad. A continuación se relacionan las conclusiones encontradas por el equipo Auditor:

1. Las directivas de la Entidad deben apropiarse y concientizarse de la importancia que representa la seguridad de la Información.

2. Es importante implementar acuerdos de confidencialidad claros y enmarcados en una normativa de repercusiones legales por el uso no autorizado de la información para funcionarios y contratistas.

3. Es primordial realizar auditorias internas enfocadas a la seguridad de la información.

CONTRALORÍA Municipal de Bucaramanga

4. Se deben contemplar capacitaciones en temas puntuales sobre seguridad de la información.

5. Se están realizando algunos procedimientos para los controles relacionados a la seguridad de la información que deben estar debidamente documentados.

6. Es relevante procurar realizar un control adecuado para el ingreso a la entidad que garantice la identificación de funcionarios, contratistas y ciudadanos.

7. Todos los archivos de gestión deben estar protegidos frente a riesgos de extracción de documentos.

8. Se debe procurar mejorar la seguridad en el acceso al rack de la red donde se encuentran los swiches y el servidor además de la seguridad para evitar extracción de equipos portátiles.

9. Se encontró cableado expuesto que es un riesgo inminente a la seguridad de la información y para los usuarios que laboran en la entidad.

10. Es relevante garantizar la recuperación efectiva y eficaz de los documentos que tiene la Entidad.

11. Es indispensable que se realicen copias de seguridad periódicas a todos los equipos de la Entidad.

Equipo Auditor:

JAIRO RINCON GARCIA
Auditor Fiscal (Líder)

ELKIN ANDRES MOLANO BARREIRO
Contratista de apoyo