Honorable Concejo Municipal de Santa Cruz de la Sierra

Resolución Municipal Nº 421/2013
á, 03 de julio de 2013

VISTOS:

El Oficio Secretaría General OF. Nº 1870/2009 de fecha 21 de Diciembre de 2009, recibido en Secretaría del Concejo Municipal en fecha 22 de Diciembre de 2009, por lo que en cumplimiento a lo establecido por el Artículo 44, Numeral 29) de la Ley Nº 2028 de 28 de octubre de 1999 – Ley de Municipalidades, se remite para consideración y Aprobación del plenario del Honorable Concejo Municipal de Santa Cruz de la Sierra, el "REGLAMENTO ESPECIFICO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMATICA PARA EL GOBIERNO AUTONOMO MUNICIPAL DE SANTA CRUZ DE LA SIERRA", y todo el expediente relativo al trámite; y,

CONSIDERANDO:

Que, la Constitución Política del Estado establece en su Artículo 302.- I.- Son competencias exclusivas de los Gobiernos Autónomos Municipales en su Jurisdicción.- Inc. 23).- Elaborar, aprobar, ejecutar sus programas de operaciones y su presupuesto.

CONSIDERANDO:

Que, la Ley 2028 de Municipales establece en su Artículo 44.- numeral 29).- El Alcalde Municipal tiene las siguientes atribuciones: Inc. 29).-Elaborar los manuales de organización, funciones, procedimientos y organigrama, para su aprobación por el Concejo.

CONSIDERANDO:

Que, la Ley 1178 SAFCO establece en su Artículo 7.- El sistema de Organización Administrativa se definirá y ajustara en función de la Programación de Operaciones. Evitara la duplicidad de los objetivos y atribuciones mediante la adecuación, fusión o supresión de las entidades (….).

***Inciso.- b).-** Toda entidad pública organizara internamente, en función de sus objetivos y la naturaleza de sus actividades, los sistemas de administración y control interno de que trata esta Ley.*

***Articulo 28.-** Todo servidor público responderá de los resultados emergentes del desempeño de las funciones, deberes y atribuciones asignados a su cargo.*

CONSIDERANDO:

Que, las Normas ISO 17799-2000, dan las pautas en la definición sobre que metodología, políticas o criterios pueden ser aplicados en el régimen de manejo de la seguridad de la información. La toma de decisiones sobre un marco de referencia de seguridad basado en esta norma, proporciona beneficios a toda organización que lo implemente.

CONSIDERANDO:

Que, las nuevas formas de comunicación e información que la Tecnología permite en estos días al implementarlas en el trabajo diario del Gobierno Autónomo Municipal, presentan nuevas actividades que exigen normas y procedimientos específicos bajo estándares internacionales para evitar contingencias e incidentes. Por este motivo es que se ve la necesidad de lograr mayores avances en temas de seguridad en el manejo de la información institucional por lo que es necesario la elaboración de un reglamento al respecto.

CONSIDERANDO:

Que, los objetivos del Reglamento se basan esencialmente en las orientaciones e instrucciones que indican cómo manejar los procesos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: Identificación y Control de Acceso, respaldo de datos, planes de contingencia y detección de intrusos. La falta de políticas y procedimientos en seguridad informática dentro del Gobierno Autónomo Municipal de Santa Cruz de la Sierra, relacionado a la protección de activos intangibles, donde se almacena la información y frente a peligros externos e internos, es necesaria la elaboración y puesta en vigencia de un Reglamento de Políticas y Procedimientos de Seguridad Informática. El presente proyecto consta de IV Títulos y 42 Artículos, que detallan las normas legales, técnicas y los conceptos básicos relativos a las políticas de seguridad informática y procedimientos. Además el proyecto contiene un anexo para la adquisición, renovación y baja de equipos, impresoras y accesorios de computación.

CONSIDERANDO:

Que, dentro del Proyecto se habla de la obligación de los funcionarios de conocer el manual de políticas, el cual debe ser entregado a cada funcionario de acuerdo al nivel que tiene, porque el acceso a la información y a los servicios de internet se propone diferenciarlo en tres niveles de acuerdo a las funciones que cada puesto requiera. Esta propuesta seria positiva para delimitar el uso de los recursos así como responsabilizar con el conocimiento de sus limitaciones a cada funcionario según sus responsabilidades.

CONSIDERANDO:

Que, otro aspecto importante de destacar es lo estipulado en el artículo 26 sobre la capacitación y actualización de todo el personal respecto a nuevos recursos informáticos y de comunicación. Así se garantizara el aprovechamiento al máximo de las inversiones realizadas por el Gobierno Autónomo Municipal en este rubro.

CONSIDERANDO:

Que, el referido proyecto de Reglamento Específico de Políticas y Procedimientos de Seguridad Informática ha sido elaborado por la Dirección de Organización y Método en coordinación con la Secretaria de Asuntos Jurídicos. Este proyecto ya ha sido consensuado y sometido a correcciones por las instancias mencionadas y está conforme a las disposiciones legales indicadas y a las necesidades actuales del Gobierno Autónomo Municipio de Santa Cruz de la Sierra. Por lo tanto, se sugiere Aprobar el Reglamento Especifico de Políticas y Procedimientos de Seguridad Informática para el Gobierno Autónomo Municipal de Santa Cruz de la Sierra.

POR TANTO:

Que, El Honorable Concejo Municipal de Santa Cruz de la Sierra, de conformidad a lo normado en la Constitución Política del Estado, del Articulo 44 numeral 29) de Municipalidades y otras normas conexa, en uso de sus legítimas atribuciones, en Sesión Ordinaria de fecha 03 de julio de 2013, dicta la siguiente;

R E S O L U C I Ó N

Articulo Primero.- *Se APRUEBA, el "REGLAMENTO ESPECIFICO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMATICA PARA EL GOBIERNO AUTONOMO MUNICIPAL DE SANTA CRUZ DE LA SIERRA", que consta de IV Títulos, 42 Artículos y 1 anexo, cuyo texto deberá formar parte de la presente Resolución*

Municipal y de lo cual deberá quedar constancia en los Archivos del H. Concejo Municipal, luego remítase al Ejecutivo Municipal para los fines de Ley.

Artículo Segundo.- *El Ejecutivo Municipal queda encargado del cumplimiento de la presente Resolución.*

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

Sr. Francisco Romel Porcel Plata
CONCEJAL SECRETARIO

Sra. María Desiree Bravo Monasterio
CONCEJALA PRESIDENTA

H. CONCEJO MUNICIPAL DE SANTA CRUZ DE LA SIERRA

GOBIERNO MUNICIPAL
SANTA CRUZ
SOMOS TODOS

"REGLAMENTO ESPECIFICO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMATICA"

APROBADO MEDIANTE RESOLUCIÓN MUNICIPAL Nº 421/2013
DE FECHA 03 DE JULIO DE 2013

Santa Cruz - Bolivia

GOBIERNO AUTÓNOMO MUNICIPAL DE SANTA CRUZ DE LA SIERRA

REGLAMENTO ESPECÍFICO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

GESTIÓN - 2009

….. o …..

REGLAMENTO ESPECÍFICO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA

TÍTULO I
NORMAS GENERALES

CAPÍTULO I
ASPECTOS GENERALES

Artículo 1.- CARACTERISTICAS GENERALES

La falta de políticas y procedimientos en seguridad informática, dentro del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, en lo que se refiere a la protección de activos de información frente a peligros externos e internos, se ve la necesidad de la elaboración del presente Reglamento de Políticas y Procedimientos de Seguridad Informática, el cual consta de IV Títulos y 42 Artículos, que detallan las normas legales, técnicas y los conceptos básicos relativos a las políticas de seguridad informática y procedimientos.

Artículo 2.- OBJETIVO DEL REGLAMENTO

El objetivo del Reglamento de Políticas y Procedimientos de Seguridad Informática, se basa esencialmente en las orientaciones e instrucciones que indican como manejar los procesos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Artículo 3.- MARCO LEGAL

El presente Reglamento de la Seguridad Informática, tiene como base jurídica el Código Penal, Capítulo XI, en sus artículos 363 Bis y 363 Ter que indican lo siguiente:

> ***Artículo 363 Bis Manipulación Informática.***
>
> *El que con la intensión de obtener un beneficio indebido para si o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio*

1. El Comité de Seguridad Informática será responsable de:

a) Elaborar y actualizar las políticas, normas, pautas, procedimientos relativos a la seguridad informática y telecomunicaciones;

b) Coordinar el análisis de riesgos, planes de contingencia y prevención de desastres.

El Comité de Seguridad Informática tendrá reuniones trimestrales donde se efectuará la evaluación y revisión de la institución en cuanto a la seguridad informática, incluyendo en el análisis los incidentes ocurridos que afectaron la seguridad.

2. El Departamento de Tecnología de Información será responsable de:

c) Implantar y velar por el cumplimento de las políticas, normas, pautas y procedimientos de seguridad informática a lo largo de todo el Gobierno Municipal Autónomo de Santa Cruz de la Sierra;

d) Evaluar, adquirir e implantar productos de seguridad informática y de realizar las demás actividades necesarias para garantizar un ambiente informático seguro;

e) Proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances;

f) Proteger y garantizar el buen funcionamiento de toda la Infraestructura Computacional y dar Seguridad a la información almacenada en los equipos del Centro de Cómputo de propiedad del Gobierno Municipal Autónomo de Santa Cruz de la Sierra.

- *El Encargado de Seguridad y Mantenimiento es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad delegando funciones al personal de seguridad y técnicos de sistemas, así como recomendar las medidas pertinentes.*

3. El Encargado de Seguridad y Mantenimiento en coordinación con el Encargado de Redes y Telecomunicaciones y el Personal de Seguridad, son los responsables de:

a) Establecer los controles de acceso apropiados para cada usuario;

y localidades en todo el Gobierno Municipal Autónomo de Santa Cruz de la Sierra, como ser: Centro de Cómputo, Edificios, Sub-Alcaldías, Etc.

4. Los Técnicos de Sistemas con el Personal de Seguridad son los responsables de Informar al Jefe del Departamento de Tecnología de Información y al Encargado de Seguridad y Mantenimiento, sobre toda actividad sospechosa o evento insólito.

5. Cuando no exista un Encargado de Seguridad, el Encargado de Redes y Telecomunicaciones en conjunto con los Técnicos de Sistemas y el Personal de Seguridad deberán realizar sus funciones.

6. Los usuarios son responsables de cumplir con todas las políticas de la Institución relativas a la seguridad informática y en particular:

a) Conocer y aplicar las políticas, procedimientos apropiados en relación al

d) No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Institución;

e) Proteger meticulosamente su contraseña y evitar que sea vista por otras personas en forma inadvertida;

f) Seleccionar una contraseña robusta que no tenga relación con el usuario, sus familiares, el grupo de trabajo y otras asociaciones parecidas. Por lo general es recomendable que sea una contraseña alfa numérica;

g) Reportar inmediatamente a su jefe inmediato o a un funcionario del Departamento de Tecnología de Información, cualquier evento que pueda comprometer la seguridad de la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

TÍTULO III
DISPOSICIONES DE SEGURIDAD

CAPÍTULO I
RIESGO Y SEGURIDAD

Artículo 11.- RIESGOS

Los riesgos son un tema importante dentro de la planificación de la administración de sistemas, ya que una vez se hacen los estudios, se pueden tomar las medidas de contingencia para evitar toda clase de problemas.

Hay que tener muy en cuenta que, al realizar el análisis de riesgo, se deben identificar ***todos*** *los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada.*

Los recursos que deben ser considerados al estimar las amenazas a la seguridad son los siguientes:

a) ***Hardware:*** *procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges, switch;*

b) ***Software:*** *programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones;*

c) ***Datos:*** *durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación;*

d) ***Gente:*** *usuarios, personas para operar los sistemas;*

e) ***Documentación:*** *sobre programas, hardware, sistemas, procedimientos administrativos locales;*

f) ***Accesorios:*** *papel, formularios, cintas, información grabada.*

Se deben realizar estudios de manera semestral para analizar todos los riesgos que se pueden presentar. Una vez identificados los riesgos se deben tomar todas las previsiones, y estudiar las más factibles para solucionar los problemas o accidentes que se pueden presentar a futuro, esto recibe el nombre dentro de la auditoria de sistemas como acción pro-activa; es decir, buscar soluciones a los problemas antes de que estos se presenten y poder tener las respuestas en estos casos.

Los pasos para poder realizar estos estudios deben ser de la siguiente manera:

a) *Se debe formar un equipo con todo el personal involucrado en el área;*

b) *Cada uno de los involucrados deben presentar los riesgos que pueden existir dentro de sus campos de acción;*

c) *Se debe tomar apunte de cada una de las presentaciones de riesgos;*

d) *Se debe de tomar cada unos de los riesgos para clasificarlos por orden de importancia o prioridad, como riesgos altos, riesgos medios y riesgos bajos;*

e) *Una vez clasificados los riesgos se debe dar las posibles soluciones y adoptar las idóneas o aptas;*

f) *Se debe llevar un registro de todos los tópicos, luego documentarlos y archivarlos para poder contar con dicha documentación en los casos de emergencia.*

En muchos casos está demostrado que la planificación de los riesgos es mejor hacerlas de manera semestral, para poder contar con planes de contingencia de corto plazo, esto

no quiere decir que no se pueden contemplar los riesgos a largo plazo, que al final pueden llegar a ser los más peligrosos, los riesgos a largo plazo también pueden ser tomados en cuenta para poder tomar planes de acción antes de que sucedan los percances durante el desarrollo de las actividades.

Artículo 12.- SEGURIDAD PARA LAS COMPUTADORAS E IMPRESORAS

Para tener una máxima seguridad de todos nuestros equipos de computación e impresoras, se deben tomar muy en cuenta los siguientes puntos:

1. *Los computadores de la Institución sólo deben usarse en un ambiente seguro, se considera que un ambiente es seguro cuando se implantaron las medidas de control apropiadas para proteger el software, hardware y los datos. Estas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles;*

2. *Los equipos de la Institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasa tiempos;*

3. *Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Tecnología de Información en cada equipo;*

4. *No se permite fumar, comer o beber mientras se está usando un equipo de computación;*

5. *Todos los equipos de computación y cualquier otro accesorio, deben estar siempre sobre muebles de oficina;*

6. *No bloquear las ranuras de ventilación de los equipos, si los equipos deben estar uno al lado del otro la distancia de separación entre ellos debería estar entre 5 y 10 cm la distancia de separación entre la parte trasera del equipo y cualquier obstáculo debería estar entre 20 y 30 cm.*

7. *Es indispensable recalcar la prudencia y el cuidado con que se debe manipular todo aparato que funcione con corriente eléctrica. Nunca deben tocar un artefacto eléctrico si usted está mojado o descalzo;*

8. *No se permitirán instalaciones eléctricas precarias o provisorias. Se dará aviso inmediato al Departamento de Servicios Generales en caso de filtraciones o goteras que puedan afectar las instalaciones o equipos y puedan provocar incendios por cortocircuitos;*

9. *Es imprescindible mantener el orden y la limpieza, cada persona es responsable directa del lugar de trabajo y de todos los lugares comunes;*

10. *Deben protegerse los equipos de los riesgos del medio ambiente (por ejemplo: polvo, agua, humedad, etc.);*

11. *Deben usarse protectores contra bajas de energía eléctrica (estabilizadores de tensión). En los servidores deben usarse fuentes de poder ininterrumpibles (UPS);*

12. *Cualquier falla en los computadores o en la red debe reportarse inmediatamente al Departamento de Tecnología de Información, ya que podría causar problemas serios, como ser pérdida de información o el mal funcionamiento de los servicios;*

13. *Deben protegerse los equipos para disminuir el riesgo de robo, destrucción o mal uso de los mismos. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave en las distintas áreas del Gobierno Municipal Autónomo de Santa Cruz de la Sierra;*

14. *Los equipos deben marcarse para su identificación y control de inventario, los registros de inventario deben mantenerse actualizados en la base de datos de bienes patrimoniales;*

15. *No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo o impresora fuera de la Institución, se requiere de una autorización escrita de su inmediato superior con una previa justificación del caso;*

16. *La pérdida o robo de cualquier componente de hardware o programa de software, equipo de computación (PC, Portátil), impresora o cualquier accesorio de computación debe ser reportado inmediatamente al Departamento de Tecnología de Información y al Departamento de Bienes Patrimoniales;*

17. *Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben habilitar manualmente el estado de bloqueado al computador con las teclas Ctrl + Alt + Supr, presionadas simultáneamente cada vez que se ausente de su oficina o la tecla con el símbolo de Windows + L;*

18. *Si una PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferentemente por hardware;*

19. *Los datos confidenciales que aparezcan en la pantalla deben protegerse, de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar;*

20. *Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario;*

21. *No está permitido llevar al sitio de trabajo computadores portátiles (laptops) de propiedad de los funcionarios municipales y en caso de ser necesario, se tiene que solicitar la autorización correspondiente;*

22. *Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems (externos o internos) en PC`s que tengan también conexión a la Red de Área Local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la Red de Área Local (LAN) de la Institución;*

23. *A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales;*

24. *No esta permitido que los usuarios utilicen el Internet para objetivos ajenos al trabajo que desempeñan, esta totalmente prohibido la descarga de material pornográfico, material nocivo para la red, juegos y software de entretenimiento por el alto contenido de virus que generalmente se descargan junto con estas aplicaciones;*

25. *Los usuarios no deben copiar a un medio removible (como ser CD, DVD, Diskette, Flash Memory), el software o los datos confidenciales residentes en las computadoras de la Institución sin la aprobación previa de un superior inmediato;*

26. *No pueden extraerse datos fuera de la sede de la Institución sin la aprobación previa de un superior inmediato. Esta política es particularmente pertinente a aquellos que usan computadoras portátiles o están conectados a redes como Internet. De la misma manera esta prohibida la transmisión de datos confidenciales por medio del correo electrónico a personas ajenas a la Institución;*

27. *Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada, si se detecta la presencia de un virus u otro agente especialmente peligroso, se debe notificar inmediatamente al Encargado de Seguridad y Mantenimiento para poner la PC en cuarentena hasta que el problema sea resuelto;*

28. *Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la institución;*

29. *No debe utilizarse ningún software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Tecnología de Información;*

30. *Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o sharewares, a menos que haya sido previamente aprobado por el Departamento de Tecnología de Información;*

31. *Para ayudar a restaurar los programas originales no dañados o infectados, se debe realizar copias de todo software antes de su uso y deben guardarse tales copias en un lugar seguro;*

32. *No deben usarse diskettes u otros medios de almacenamiento como CD, DVD o Flash Memorys, en cualquier computadora de la institución a menos que haya sido previamente verificado que estén libres de virus u otros agentes dañinos;*

33. *No se debe copiar información de una computadora a otra en medios de almacenamiento como diskettes, CD, DVD o Flash Memorys sin que haya sido previamente revisado que estén libres de virus u otros agentes dañinos;*

34. *Periódicamente debe hacerse los respaldos, de los datos guardados en los PC's y servidores, las copias de respaldo deben guardarse en un lugar seguro a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de institución deben guardarse en otra sede, lejos del edificio;*

35. *Los usuarios de los computadores son los responsables de proteger los programas y datos contra pérdida o daño; mientras que para los sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es*

responsable de hacer copias de respaldo periódicas. Los jefes de los distintos Departamentos son responsables de definir que información debe protegerse contra pérdida y la frecuencia de la realización de esta operación, (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total). Si los usuarios no cuentan con los medios de hardwares como ser quemadores de CD o DVD, deben solicitar al personal del Departamento de Tecnología de Información que les realicen la copia de la información previamente seleccionada por los usuarios y previa autorización de un superior inmediato;

36. *La información de la Institución clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas robustas de encriptado que hayan sido aprobadas por el Jefe de Departamento de Tecnología de Información;*

37. *No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado;*

38. *No debe formatearse ningún equipo de computación, instalar sistema operativo o aplicaciones, mover equipos e impresoras, desconectar y conectar cables de red y corriente de un equipo (PC, Portátil, Impresoras, Scanner y otros) o equipos de comunicación (switch, router, modem, rack, etc.) a otro lugar, sin previa autorización del Jefe del Departamento de Tecnología de Información;*

39. *El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas, en ningún caso deben revelarse a consultores, contratistas o personal temporal;*

40. *Siempre que sea posible, debe eliminarse la información confidencial de los computadores y/o unidades de disco duro antes de que se han enviadas a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, se debe efectuar la reparación bajo la supervisión de un representante de la institución;*

41. *No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo o se va a imprimir, información confidencial de la Institución. Se debe tener especial cuidado en la impresión de planillas de pago y la impresión de cheques de tesorería, para evitar perdidas de documentos;*

42. *El personal que utiliza un computador portátil que contenga información confidencial de la Institución, debe tener la información cifrada y no debe dejarla desatendida y tener aun más cuidado si se encuentra de viaje;*

43. *Los equipos portátiles al momento de sacarlos fuera de la institución, con el permiso necesario de un inmediato superior, deben hacerlo siempre dentro de un maletín, evitando así polvo, humedad, agua, etc. que pueda dañar el funcionamiento del equipo y pérdida de información;*

44. *Cuando un usuario cambie de área, el equipo asignado a este deberá permanecer dentro del área designada originalmente. Sera responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle el equipo de computo requerido para el desarrollo de sus funciones. Para realizar la Transferencia de equipos, impresoras y accesorios de computación el usuario deberá solicitar por vía escrita al Departamento de Bienes Patrimoniales el traslado de las mismas para un nuevo usuario;*

45. *De acuerdo a los lineamientos de reducción de costos, optimización y eficiencia de los recursos, los bienes informáticos y periféricos de computo personal usados podrán ser reciclados y asignados a un usuario antes de que estos se vuelvan obsoletos;*

46. *Las impresoras laser blanco/negro o de color de red asignadas, tendrán uso compartido por un grupo de usuarios o también de uso personal pero justificado, el resguardo de la misma es responsabilidad del usuario más cercano al equipo;*

47. *Las impresoras laser blanco/negro o de color de red deberán estar instaladas en lugares abiertos y accesibles para que los usuarios no tengan ningún problema en utilizarlas;*

48. *La asignación de una impresora en red, será de acuerdo a la justificación plena por cargas de trabajo del área usuaria y a la capacidad de impresión de esta última;*

49. *Los equipos de digitalización (scanner) solo serán asignados a usuarios que por su función del puesto así lo requieran y deberá ser solicitado por escrito donde se describa la justificación y deberá ser autorizado por su inmediato superior.*

Artículo 13.- SEGURIDAD PARA USO ADECUADO DEL INTERNET, COMUNICATOR Y MESSENGER

El Departamento de Tecnología de Información es el encargado de autorizar y brindar permisos a todos los usuarios del Gobierno Municipal Autónomo de Santa Cruz de la Sierra para acceso a Internet, Comunicator y Messenger, previa verificación escrita de autorización enviada al Jefe del Departamento de Tecnología de Información, vía Oficialía Mayor de Administración y Finanzas. Los usuarios deben cumplir con las siguientes recomendaciones:

1. *Está prohibido usar el Comunicator y Messenger para objetivos ajenos al trabajo que desempeñan cada funcionario dentro de la institución;*
2. *Antes de realizar una transferencia de archivos ya sea por Comunicator o Messenger se debe realizar una revisión de virus con algún software de antivirus instalado, antes de ser enviado al destinatario. Si el equipo no tiene algún software de antivirus instalado, el usuario debe reportar al Encargado de Mantenimiento y Seguridad para su inmediata instalación;*
3. *Cuando un usuario no se encuentra en su lugar de trabajo, se debe cambiar de estado (Disponible, Ausente, Ocupado, No Molestar, Vuelvo enseguida) tanto en el Comunicator y en el Messenger;*
4. *Cada persona es responsable de su Cuenta y Password de Usuario, ya que es de uso confidencial;*
5. *Está prohibido que los usuarios utilicen el Internet para objetivos ajenos al trabajo que desempeñan, la descarga de material pornográfico, material nocivo para la red, juegos y la descarga de cualquier software de entretenimiento (video, mp3, drivers) por el alto contenido de virus al momento de la descarga;*
6. *Algunos sitios de Internet se encuentran bloqueados (facebook, youtube, etc.) ya que no contribuyen a funciones laborales de los usuarios, cualquier excepción para otorgar permiso de acceso a estos sitios restringidos se deberá hacer por escrito al Jefe del Departamento de Tecnología de Información vía el Oficialía Mayor de Administración y Finanzas, previa autorización y justificación de su inmediato superior;*
7. *Los mensajes que se envíen vía Internet, será de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra institución;*
8. *Está prohibido inspeccionar, copiar y almacenar programas computacionales, software y demás material electrónico que violen la ley de derechos de autor;*

9. *Está prohibido la descarga de programas "point to point" (P2P) para bajar archivos de música o videos desde Internet, los cuales ocupan en demasía el ancho de banda del Gobierno Municipal Autónomo de Santa Cruz de la Sierra;*
10. *Queda prohibido otorgar acceso a personas ajenas a la institución, para que revisen sus correos electrónicos gratuitos (Hotmail, Yahoo, Gmail, Etc.) y acceso al Messenger en los equipos de propiedad del Gobierno Municipal Autónomo de Santa Cruz de la Sierra.*

Artículo 14.- SEGURIDAD PARA USO ADECUADO DEL CORREO INSTITUCIONAL (GMSANTACRUZ.GOV.BO)

El Departamento de Tecnología de Información es el encargado de la creación de cuentas de usuario y autorización de permisos para acceso al Correo Institucional del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, previa verificación escrita de autorización enviada al Jefe de Departamento de Tecnología de Información. Los usuarios deben tomar las siguientes recomendaciones:

1. *El uso del Correo Institucional es para fines de carácter netamente laboral;*

2. *Al momento de enviar un correo con algún Archivo Adjunto, este debe ser analizado por un Software de Antivirus antes de su respectivo envió al destinatario;*

3. *Está prohibido enviar correo electrónico con Información Confidencial a personas que no tengan ningún vinculo laboral con la institución;*

4. *Es responsabilidad del usuario mantener la confidencialidad de su clave de acceso;*

5. *La cuenta de correo es personal e intransferible no permitiéndose que segundas personas hagan uso de ella;*

6. *Cada usuario es el responsable de las acciones efectuadas en su cuenta;*

7. *El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión o posterior baja del sistema del servicio;*

8. *Es responsabilidad del usuario limpiar su cuenta periódicamente para que exista espacio disponible;*

9. *Todo usuario es responsable por los correos y archivos adjuntos que reciba, si algún correo electrónico tiene contenido extraño o duda de su recepción, el usuario no debe abrir dicho correo, puede contener virus que afectaría el funcionamiento del equipo o perdida de información;*

10. *Se asignara solamente una cuenta por usuario con un espacio determinado:*

    a. ***Cuenta Personal:*** *asignadas a las personas solicitantes en forma individual. El nombre de la cuenta consiste en la inicial del nombre seguida por el apellido, completando entre ambos un máximo de quince (15) caracteres. Por ejemplo, si una persona se llama Juan Perez, su cuenta de correo será jperez@gmsantacruz.gov.bo. En el caso de que el apellido sea muy largo se cortara hasta completar el máximo.*

    b. ***Casos especiales de Cuentas Personales:*** *En el caso que dos o más personas coincidan en la inicial del nombre y en el apellido, el primero que solicite cuenta se le dará con el formato anterior, y a las siguientes se les agregara la siguiente letra de su nombre, completando igualmente los quince caracteres máximos con el apellido. Por ejemplo: Mauricio Orellana, morellana, maorellana, mauorellana, etc. y si aún así coinciden se deberá agregar letras del segundo apellido.*

11. *Cuando un usuario escriba un mensaje a alguien que no conoce, preséntese siempre, indicando como se llama y quien es, y por supuesto firme sus mensajes;*

12. *Si se quiere enviar un correo a varias personas, utilizar el campo "CC" o "BCC" para escribir las direcciones. Así se evita que se conozcan las direcciones del resto de la lista;*

13. *Queda prohibido inscribirse a listas de correos o de servidores, las cuales no estén relacionadas directamente con su trabajo por motivos de que algunas listas de correo o de servidores generan cantidades masivas de correos a los subscriptores. Esto no solamente satura el espacio disponible en el disco duro de la estación de trabajo, sino que también degrada el funcionamiento del sistema de email entero;*

14. *El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS (Correos masivos no autorizados) de información, ni de mandar anexos que pudieran contener información nociva para otro usuario como virus, juegos o pornografía;*

15. *Si un usuario desea enviar email al correo global del municipio, debe hacer llegar de forma escrita una solicitud firmada por su inmediato superior al Jefe del Departamento de Tecnología de Información vía Oficialía Mayor de Administración y Finanzas con su debida justificación del caso;*

16. *Está expresamente prohibido enviar mensajes no solicitados ("correo basura" o "spam") del tipo que sea (publicidad comercial, proclamaciones políticas, anuncios personales, etc.) tanto al correo personal de cada funcionario, como al correo global del municipio;*

17. *Se entiende por spam, todo correo que se envié masivamente a través del servidor de correo, que represente un riesgo de saturar la cola de correos, así como la operación del servicio de correo ante entidades nacionales y/o internacionales, afectando así el uso normal de los servicios a los demás usuarios;*

18. *A los usuarios no les está permitido reenviar o propagar mensajes encadenados ni correo electrónico malintencionado, entendiéndose como tal a manera de ejemplo pero no limitativa, la suplantación de identidades, propagación de virus, correos que atenten contra la integridad de terceros, ataque de directorio, entre otros;*

19. *Los usuarios no podrán acceder a los mensajes de direcciones de correo electrónico que no sean las suyas propias, a menos que cuenten con el pleno consentimiento del dueño de la dirección en cuestión.*

Artículo 15.- SEGURIDAD EN REDES, EQUIPOS DE COMUNICACIÓN Y EQUIPOS DE APOYO

El Término de Seguridad en Redes, es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Los equipos de comunicación como los equipos de apoyo también necesitan ciertas normas de seguridad, para evitar los problemas de mal funcionamiento.

Los equipos de comunicación necesitan contar con las mismas características de seguridad que los demás equipos, desde la instalación hasta la misma puesta en funcionamiento, además es también necesario colocar estos equipos en lugares donde se encuentren de manera fija y sin peligro de accidentes o caídas, los cables de conexión deben ser fijados de tal manera que no queden sueltos y se produzcan problemas de pérdida de comunicación. Como complemento se debe realizar un mantenimiento periódico, tanto físico como lógico de estos equipos, para poder garantizar un buen

funcionamiento, esta tarea también se debe realizar a todos los cableados y tomas de las redes.

Los materiales del cable, la categoría y el tendido de fibra deben estar de acuerdo con los estándares de cableado estructurado según las normas ISO y TIA-EIA.

Los equipos de apoyo como son los estabilizadores y UPS deben contar también con una debida instalación eléctrica para un correcto funcionamiento, esta instalación debe ser supervisada y revisada periódicamente por un especialista en la materia.

Artículo 16.- SEGURIDAD EN REDES INALAMBRICAS O WIRELESS

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Las redes inalámbricas (Wireless) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. Es una red que permite a sus usuarios conectarse a una red local o a Internet sin estar conectado físicamente, sus datos (paquetes de información) se trasmiten por el aire. La recepción y la transmisión se realizan a través de antenas. Al montar una red inalámbrica hay que contar con un PC que sea un "Punto de Acceso" y los demás son "dispositivos de control", toda esta infraestructura puede variar dependiendo que tipo de red queremos montar en tamaño y en la distancias de alcance de la misma. Las siguientes políticas de seguridad se deben tomar en cuenta:

a) *El Standart IEEE 802.11 implementó un mecanismo para proteger a los usuarios autorizados de una red WLAN de las escuchas ocasionales, denominado Wired Equivalent Privacy (WEP). El Standart WEP de IEEE 802.11 especifica una clave de 128 Bits o más, siendo esta la longitud mínima*

necesaria para un esquema de trabajo seguro. Cuando se usa WEP (Wireless Equivalent Privacy), tanto el cliente inalámbrico como el Access Point deben tener una clave WEP idéntica;

b) *Habilitar los mismos parámetros de configuración WEP en los clientes. Una vez completado este paso permitiremos a las tarjetas de red comunicarse con el punto de acceso inalámbrico compartiendo los mismos parámetros de configuración con el punto de acceso;*

c) *Utilizar claves WEP no triviales y cambiarlas regularmente. Los consejos a la hora de elegir una contraseña son bien conocidos; como norma general no elegir datos personales que otras personas puedan conocer o averiguar (nombre mascota, año de nacimiento, N°de CI, Etc.) También hay que ir con mucho cuidado de no elegir cualquier palabra que pueda aparecer en un diccionario ya que puede resultar muy fácil para un ordenador averiguarla por fuerza bruta;*

d) *No utilizar TCP/IP para compartir archivos e impresoras. Si algún intruso consigue conectarse a nuestro punto de acceso, estará dentro de nuestra red LAN como cualquier otro cliente legítimo, esto quiere decir que estará utilizando el protocolo TCP/IP en su conexión, y con esta opción activada no podrán acceder a nuestra información privada. De este modo deberemos utilizar otro protocolo para hacer uso de la compartición de archivos e impresoras (Ej. NetBEUI);*

e) *Establecer autentificación compartida. La autentificación compartida, se refiere al método de autentificación por clave compartida, que aunque no es el más seguro del mundo resulta más conveniente que dejar la autentificación abierta. Este parámetro puede ser establecido en las propiedades avanzadas de nuestro punto de acceso que debe aparecer como "Shared Key";*

f) *Ocultar el SSID. Esta medida nos protegerá de posibles intrusos que puedan descubrir de manera sencilla nuestra red, y como consecuencia, puedan aprovecharse de ella o bien intentar atacarla para dejarla fuera de servicio. En el punto de acceso esto se consigue habilitándolo en modo pasivo, (ya explicado anteriormente) y para conseguir esto se establecerá como falso el parámetro "SSID broadcast";*

g) *Cambiar las claves por defecto cuando instalemos el software del punto de acceso;*

h) Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red;

i) Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto más de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro;

j) Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de trasmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

CAPÍTULO II
SEGURIDAD PARA LAS COMUNICACIONES

Artículo 17.- PROPIEDAD DE LA INFORMACIÓN

Los Sistemas de Comunicación de la Institución generalmente deben usarse para actividades de trabajo, el uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo, recursos, y además no interfiera con la productividad del funcionario, ni con las actividades de la Institución.

Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión. De la misma manera, no se podrá realizará la navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución.

Artículo 18.- CONFIDENCIALIDAD Y PRIVACIDAD

No debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrados bajo la supervisión del personal del Departamento de Tecnología de Información.

Los funcionarios de la Institución no deben interceptar las comunicaciones o divulgar su contenido, tampoco deben ayudar a otros para que lo hagan.

Si un usuario olvida por accidente cerrar su sesión de correo electrónico, ningún otro funcionario debe leer el contenido de éste, respetando así la privacidad de cada uno como persona.

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento, con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

CAPÍTULO III
SEGURIDAD PARA REDES

Artículo 19.- CUENTA DE LOS USUARIOS

Cuando un usuario recibe una cuenta nueva, debe recibir el manual de Políticas de Seguridad Informática y firmar un documento donde declarará haber recibido el manual y hacerse responsable de respetar cada una de las políticas que este contenga, así como aceptar sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una nueva cuenta de usuario para acceso al dominio, navegación a internet, comunicator, correo institucional o el cambio de privilegios debe ser realizada por escrito al Jefe del Departamento de Tecnología de Información vía la Oficialía Mayor de Administración y Finanzas, previa autorización de su inmediato superior. En caso de acceso a Internet se debe especificar el nivel de acceso para navegación:

1. ***Nivel Básico:*** *solo ingreso a paginas .gov.bo;*
2. ***Nivel Medio:*** *navegación irrestricta, sin acceso al Messenger;*
3. ***Nivel Avanzado:*** *navegación irrestricta con acceso a Messenger (solo oficiales y directores).*

Tampoco debe concederse una cuenta a personas que no sean empleados de la Institución a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al fin de las actividades para las cuales esa cuenta debió ser creada.

Los privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

Se prohíbe el uso de cuentas anónimas o de invitado (guest), los usuarios deben entrar al sistema mediante cuentas que identifiquen claramente su identidad. Esto también implica que los administradores de sistemas (Sistema Operativo del PC), no deben entrar inicialmente como "root" (Directorio Raíz), sino primero empleando su propio

Identificador (ID) y luego mediante "set userid" (Comando del Sistema Operativo del PC), para obtener el acceso como "root"(Directorio de Raíz).

En cualquier caso debe registrarse en la bitácora (Listados de Sucesos) todos los cambios del Identificador (ID). Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa sus funciones.

En los casos que un empleado es despedido o renuncia a la institución, debe desactivarse su cuenta al momento de dejar su cargo.

Artículo 20.- CONTRASEÑAS Y CONTROL DE ACCESO

Se deben seguir los siguientes pasos para tener una mayor seguridad con respecto a contraseñas y controles de acceso:

1. *El usuario que posee una cuenta dentro del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, no debe guardar su contraseña en una forma legible como ser: en el archivo de un disco, tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. Tampoco deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores;*

2. *Nunca debe compartirse la contraseña o revelarla a otros, el hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña;*

3. *Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador;*

4. *La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión, en ese momento, el usuario debe escoger otra contraseña;*

5. *Las contraseñas predefinidas que traen los equipos nuevos tales como routers (es un dispositivo hardware o software de interconexión de redes de computadoras que opera en el nivel de red, este dispositivo interconecta segmentos de red o redes enteras), switchs (es un dispositivo electrónico de interconexión de redes de computadoras que opera en el nivel de enlace de datos), etc., deben cambiarse inmediatamente al ponerse en servicio el equipo;*

6. *Para prevenir ataques, cuando el software del sistema lo permite, debe limitarse el número infructuoso consecutivo de introducción de la contraseña a tres intentos, quedando la cuenta involucrada suspendida, debe alertar al Administrador del Sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada;*

7. *Si el sistema de control de acceso no está funcionando apropiado, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado;*

8. *Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso al sistema, acciones de esta naturaleza se consideran violatorias de las políticas de la institución, pudiendo ser causal de despido del Gobierno Municipal Autónomo de Santa Cruz de la Sierra;*

9. *Para tener evidencias de malos manejos de información y llevar a cabo acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos;*

10. *Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas;*

11. *Los servidores de red y los equipos de comunicación deben estar ubicados en espacios apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estas áreas y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo: acceso por medio de huellas digitales o tarjetas de seguridad);*

12. *El encargado de Seguridad y Mantenimiento debe tener un registro formal de todas las personas registradas para utilizar los servicios.*

Artículo 21.- ADMINISTRACIÓN DE PRIVILEGIOS

El Encargado de Mantenimiento y Seguridad en coordinación con el Encargado de Redes y Telecomunicaciones; y el Encargado de Base de Datos deben limitar y controlar la asignación y uso de privilegios, (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). Deben identificarse los privilegios asociados a cada producto del sistema (por ejemplo: sistema operativo, sistema de administración de bases de datos y aplicaciones) y las categorías de personal a las cuales deben asignarse los productos.

Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento. Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.

Artículo 22.- REFERENTE A LOS CONTRATOS CON TERCEROS

El contrato para los servicios terciarios debe garantizar que no surjan malentendidos entre la Institución y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor.
Los acuerdos de tercerización deben contemplar los riesgos, controles de seguridad y procedimientos para sistemas de información, redes y/o ambientes de PC desktop environments (ambientes de escritorio) en el contrato entre las partes.

La Empresa Terciaria como mantenimiento de hardware y software deben quedar ajustados a las políticas de seguridad de la institución, especialmente en lo que a controles se refiere.

Artículo 23.- OBLIGACIONES DE LA EMPRESA TERCIARIA

Para tener mayor control, la Empresa Terciaria está obligada a:

a) *Entregar notas de recibo o exigir notas de salida de hardware por parte del Departamento de Tecnología de Información;*

b) *Tener total disponibilidad y contar con la integridad necesaria para tratar con datos confidenciales;*

c) *Describir claramente todos los servicios que ofrecen para tomar las medidas de seguridad que correspondan;*

d) Informar del cambio y despido de personal que efectúe durante el tiempo que presten servicios a la institución, para evitar posibles hurtos y accesos no deseados;

e) Contemplar en su haber empresas de mantenimiento de hardware y software, seguridad, limpieza y mensajería por así decir, deben portar su respectiva identificación en un área visible para transitar en los predios de la institución, deben estar debidamente registrados por el Dirección de Recursos Humanos para controlar el acceso a las diferentes áreas del Municipio;

f) Responder sobre la información contenida en los PC´s que se encuentren a su cargo. Queda explicito que ellos deben hacer uso de sus propias Políticas de Seguridad Informática;

g) Mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo;

h) Garantizar al Departamento de Tecnología de Información que los PCs, son entregados luego de las revisiones periódicas libres de software malicioso, si esto no se cumpliría sería tomado como un atentado a la seguridad del Gobierno Municipal Autónomo de Santa Cruz de la Sierra y sometido a las sanciones legales que correspondan.

Artículo 24.- PROHIBICIONES DE LA EMPRESA TERCIARIA

Por razones de seguridad la Empresa Terciaria tiene las siguientes prohibiciones:

a) Esta prohibida la extracción de equipos, información y software de los discos duros sin la respectiva autorización del Departamento de Tecnología de Información;
b) No podrá realizar modificaciones en la configuración de los sistemas instalados por el Departamento de Tecnología de Información, así como cualquier modificación de los datos contenidos en los discos duros de los PC's que queden a su cargo;
c) Se prohíbe la copia y divulgación de información por parte de terciarios, con pena a sanción legal y pérdida de contrato;
d) Las empresas de mantenimiento no tienen autorización para instalar software a los PC's sin una debida autorización del Departamento de Tecnología de Información.

Artículo 25.- MANEJO DE LA INFORMACIÓN FÍSICA

La información debe ser clasificada para señalar la necesidad, las prioridades y el grado de protección.

Dicha información tiene diversos grados de sensibilidad y criticidad. Algunos ítems pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

Las cintas magnéticas, son cintas plásticas de varias capas una de las cuales esta impregnada con partículas magnéticas, generalmente es utilizada para grabación de datos. Estas cintas magnéticas de backup deben ser guardadas en condiciones altas de seguridad, es decir bajo llave, y tener copias del mismo backup en un lugar que no sean los predios del Municipio, para que en caso de desastres naturales como incendios o inundaciones se puedan restablecer los sistemas con la información intacta. Se debe crear un sistema de archivo efectivo para el almacenamiento de la información.

Cuando corresponda, los documentos en papel y los medios informáticos deben ser almacenados bajo llave en gabinetes y otro tipo de mobiliario seguros, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

Artículo 26.- FORMACIÓN Y CAPACITACIÓN EN MATERIA DE SEGURIDAD INFORMÁTICA

Todos los empleados de la institución deberán recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos del Municipio, esto comprende los requerimientos de seguridad, las responsabilidades legales y controles de la Institución, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, por ej. el procedimiento de entrada al sistema "log-on" (Identificador de usuario, contraseña o reconocimiento de voz) y el uso de paquetes de software, antes de que se les otorgue acceso a la información o a los servicios.

Artículo 27.- SEGURIDAD DEL EQUIPAMIENTO EN EL ÁREA DE SERVIDORES

El equipamiento del área de servidores debe ser ubicado o protegido de tal manera que se reduzcan los riesgos, amenazas, peligros ambientales y oportunidades de acceso no autorizado. Estos servidores deben estar ubicados en un lugar cerrado y con acceso permitido solo al personal especializado por medio de controles magnéticos, como huellas digitales y tarjetas electrónicas.

El área de servidores debe contar con todos los estándares de cableado de red y eléctrico y para evitar las radiaciones electromagnéticas, torceduras que incrementen la

atenuación, etc. Se debe asegurar el área para evitar el polvo, vibraciones, efectos químicos o agua.

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas; se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos. Para garantizar el suministro de energía se debe contar con múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía y suministro de energía ininterrumpible (UPS).

Artículo 28.- LA SEGURIDAD DEL CABLEADO DE RED

Los materiales del cable, la categoría y el tendido de fibra óptica deben estar de acuerdo con los estándares de cableado estructurado según las normas ISO y TIA-EIA; tanto para el cableado interior (intra building, significa cableado dentro de un edificio o espacio cerrado) como para exteriores. El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo: mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas. Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

Artículo 29.- BAJA O REUTILIZACIÓN DE LOS EQUIPOS

Todos los elementos del equipamiento que contengan dispositivos de almacenamiento, (por ejemplo: discos rígidos no removibles), deben ser controlados para asegurar que todos los datos sensitivos y el software bajo licencia, han sido eliminados o sobrescritos antes de su baja.

Se debe realizar un análisis de riesgo a fin de determinar si los medios de almacenamiento dañados, contienen datos sensitivos, estos deben ser destruidos, reparados o desechados.

Artículo 30.- PROCEDIMIENTO DE MANEJO DE INCIDENTES

Se debe establecer responsabilidades y procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

El Encargado de Mantenimiento y Seguridad de Redes debe delegar funciones a su personal de seguridad asignado. Corresponde a tal efecto instaurar procedimientos (planes de contingencia) que contemplen todos los tipos probables de incidentes relativos a seguridad, incluyendo:

a) Fallas en los sistemas de información y pérdida del servicio;

b) Negación del servicio;

c) Errores ocasionados por datos incompletos o inexactos;

d) Violaciones de la confidencialidad;

e) Caídas de servidores.

También está dentro del Procedimiento del Manejo de Incidentes la correcta planificación e implementación de soluciones para evitar la repetición del mismo incidente. Al mismo tiempo, comunicar a las personas afectadas o involucradas con la recuperación del mencionado incidente.

Todas las acciones de emergencias deben ser documentadas en forma detallada y comunicadas al Jefe del Departamento de Tecnología de Información y revisarse sistemáticamente.

Artículo 31.- SEPARACIÓN ENTRE INSTALACIONES DE DESARROLLO E INSTALACIONES OPERATIVAS

Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo. El software en desarrollo y en operaciones debe, en la medida de lo posible, ejecutarse en diferentes procesadores o en diferentes dominios o directorios. Cuando no es requerido, los compiladores, editores y otros utilitarios del sistema no deben ser accesibles desde los sistemas que están los operativos.

Se deben utilizar diferentes procedimientos de conexión "log-on" (Procedimientos de entrada a un sistema, contraseña o reconocimiento de voz) para sistemas en operaciones y de prueba, a fin de reducir el riesgo de error. Alentar a los usuarios a utilizar diferentes contraseñas para estos sistemas, y los menús deben desplegar adecuados mensajes de identificación.

Artículo 32.- SEGURIDAD DE LA DOCUMENTACIÓN DE SISTEMAS

La documentación del sistema puede contener cierta cantidad de información sensible (por ejemplo: descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización), por lo que la documentación del sistema debe ser almacenada en forma segura. De la misma manera debe procederse con la documentación de configuración y mapeo de redes, análisis de sistemas y estructuras de las bases de datos.

CAPÍTULO IV
REALIZACIÓN DE BACKUPS DE INFORMACIÓN

Artículo 33.- DATOS QUE DEBEN SER COPIADOS

Se tiene que realizar Backups (copia de ficheros o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales) del sistema operativo. En caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos.

Conviene efectuar backups del software base; paquetes y/o lenguajes de Programación con los que fueron desarrollados o interactúan los aplicativos institucionales.

Corresponde realizar backups del software aplicativo; considerando tanto los programas fuentes, como los programas ejecutables correspondientes, y cualquier otro software o procedimiento que también trabaje con la información, para producir los resultados con los cuales trabaja el usuario final.

Se deberán efectuar backups de los datos; bases de datos, índices, tablas de validación, palabras claves y todo archivo necesario para la correcta ejecución del Software Aplicativo.

*Las **copias de seguridad** son un proceso que se utiliza para salvar toda la información, es decir, un usuario, quiere guardar toda la información, o parte de la información, de la que dispone en el PC hasta este momento, realizará una copia de seguridad de tal manera, que lo almacenará en algún medio de almacenamiento tecnológicamente disponible hasta el momento como por ejemplo: cinta, DVD, BluRay, en discos virtuales que proporciona internet o simplemente en otro disco duro, para posteriormente si pierde la información, poder restaurar el sistema.*

La copia de seguridad es útil por varias razones:

1. *Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema);*

2. *Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos);*

3. *En el mundo de la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos. Por ejemplo, en España la Agencia Española de Protección de Datos (AEPD).*

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas, si bien dependiendo de lo que se trate podrían usarse disquetes, CD, DVD, Discos ZIP, JAZ o magnético - ópticos, pendrives o pueden realizarse sobre un centro de respaldo remoto propio o vía internet.

La copia de seguridad puede realizarse sobre los datos, en los cuales se incluyen también archivos que formen parte del sistema operativo. Así las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos, y se convierten por lo tanto en el último recurso a utilizar.

Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas. Esta capacidad puede llegar a ser algo muy importante, incluso crítico, para las empresas. Se han dado casos de empresas que han llegado a desaparecer ante la imposibilidad de recuperar sus sistemas al estado anterior a que se produjese un incidente de seguridad grave.

Artículo 34.- DEL HARDWARE PROPICIO PARA OBTENER LOS BACKUPS

Los backups se almacenarán en el mismo servidor y en diferentes tipos de cintas magnéticas, su uso dependerá del drive (dispositivos de entrada y salida de datos del PC o Server) que tiene el equipo de donde se obtendrá el backup.

Rotulación de las cintas magnéticas:

1. *Cada cinta deberá ser etiquetada usando un código sencillo que indique a que lugar del sistema de backup pertenece y con un número de secuencia;*

2. *La etiqueta para las cintas de backup diario tendrá el nombre del servidor seguido de un número secuencial;*

3. *La etiqueta para las cintas de backup semanales tendrá el nombre del servidor seguido de la letra "S" y un número;*
4. *La etiqueta para las cintas de backup mensuales tendrá el nombre del servidor seguido de la letra "M" y un número.*

Registro de cintas magnéticas:

1. *Se tendrá un registro escrito y uno electrónico de todas las cintas. Un registro para las cintas de backups diarios, semanales y mensuales y un registro diferente para las cintas de backups anuales;*

2. *Para el registro electrónico se registrará el área a la que pertenecen los servidores, los servidores de los que se saca backup, el número de cinta, y la fecha en que fue usada cada cinta;*

3. *Para el registro manual se realiza un registro por servidor donde se registran las cintas por fecha.*

Artículo 35.- SOFTWARE DE BACKUP QUE SE UTILIZARÁ

El Software es una serie de instrucciones y datos, que permite aprovechar todos los recursos que el computador tiene, de manera que pueda resolver gran cantidad de problemas.

Se utilizará el software para empaquetar cada servidor y los utilitarios de la base de datos para obtener los respaldos correspondientes.

Artículo 36.- TIPO DE BACKUP Y LA FRECUENCIA DE LOS MISMOS

Se obtendrán backups manuales utilizando un menú de operador presente en cada servidor o mediante crones programados.

Los tipos de backup que se utilizarán son:

1. ***Backup Global.*** *Se realiza una copia de toda la base de datos y de todas las aplicaciones;*

2. ***Backup Incremental.*** *Se realiza una copia de los archivos que han cambiado desde el backup anterior;*

3. ***Backup Simultáneos.*** *Se realiza en el backup manual una copia de la base de datos en otros servidores. En este caso se tiene dos respaldos para las bases de datos de Producción:*

    - *Copia en servidor Help Desk (ayuda técnica dirigida al usuario);*
    - *Copia de contingencia.*

4. ***Backup Temporal.*** *Se realiza en el backup manual una copia de la base de datos de producción en el mismo servidor.*

Los backups de las bases de datos se obtendrán diariamente, a partir de la una de la mañana. Los backups de las aplicaciones se obtendrán diariamente en horas de la noche,

cuando no existan usuarios en ninguna aplicación. Se realizarán backups semanales, mensuales y anuales.

Artículo 37.- LUGAR DE ALMACENAMIENTO DE LOS BACKUPS

Las cintas magnéticas se almacenarán en el Centro de Cómputo ubicado en el Departamento de Tecnología de Información, en un almacén bajo llave y en la caja de seguridad de alguna entidad financiera o banco. Las cintas diarias se almacenarán por una semana, las semanales se almacenarán hasta 5 semanas y las mensuales y anuales serán permanentes.

Artículo 38.- ESTABLECIMIENTO DE UN PROCEDIMIENTO PARA LA VERIFICACIÓN DE LOS BACKUPS

Diariamente se verificará que los backups se hayan obtenido correctamente, que los archivos de backup estén almacenados en los servidores y se leerán las cintas para determinar si los backups se grabaron correctamente.

Artículo 39.- DETERMINACIÓN DE LAS PERSONAS QUE OBTENDRÁN LOS BACKUPS Y REALIZARÁN LA VERIFICACIÓN

El backup será obtenido manualmente por el operador de turno nocturno, y será verificado por el operador de turno diurno.

TÍTULO IV
DE LOS PROCEDIMIENTOS Y RESPONSABILIDADES

CAPÍTULO I
PROCEDIMIENTOS

Artículo 40.- PROCEDIMIENTO DE ALTA DE CUENTA DE USUARIO

Cuando un funcionario del Gobierno Municipal Autónomo de Santa Cruz de la Sierra requiera una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

- *Nombre y Apellido;*
- *Cargo y Puesto de trabajo;*
- *Visto Buenos del Jefe inmediato superior avalando el pedido;*
- *Descripción de los trabajos que debe realizar en el sistema;*

- *Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de "buen uso de los recursos";*

- *Explicaciones breves, pero claras de cómo elegir su Password.*

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

- *Tipo de cuenta;*

- *Fecha de caducidad;*

- *Fecha de expiración;*

- *Datos referentes a los permisos de Acceso de Internet:*

    - *Nivel Básico.- solo ingreso a paginas .gov.bo;*

    - *Nivel Medio.- navegación irrestricta, pero sin ingreso a Messenger;*

    - *Nivel Avanzado.- navegación irrestricta incluido Messenger.*

Artículo 41.- PROCEDIMIENTO DE BAJA DE CUENTA DE USUARIO
Este procedimiento es el que se llevará a cabo cuando un funcionario se ausenta de la organización o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de aucensias: permanente y parcial.

Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la política de seguridad, debe estar fuertemente apoyado por parte de las autoridades del Gobierno Municipal Autónomo de Santa Cruz de la Sierra.

Ante el alejamiento y/o ausencia de un usuario de la institución; la Dirección de Recursos Humanos, deberá informar en un formulario de "Ausencia y/o Alejamiento de Personal", los siguientes datos:

- *Nombre y Apellido;*
- *Cargo que ocupaba y Puesto de Trabajo;*
- *Tipo de alejamiento (Temporal o Permanente).*

Una vez llegada la información al Departamento de Tecnología de Información, esta será utilizada para dar de baja o inhabilitar la cuenta del usuario.

La definición de baja o de inhabilitar; es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción. Si el alejamiento y/o ausencia del individuo no era permanente, al volver a la Institución, la Dirección de Recursos Humanos deberá comunicar su regreso, por medio de un formulario dando cuenta de tal hecho al Departamento de Tecnología de Información para volver habilitar la cuenta al usuario.

CAPÍTULO II
RESPONSABILIDADES AL INCUMPLIMIENTO

Artículo 42.- RESPONSABILIDADES AL INCUMPLIMIENTO DE NORMAS VIGENTES. *Los Funcionarios Municipales y en especial el Departamento de Tecnología de Información dependiente de la Dirección de Organización Métodos y Tecnología del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, que incumplan las disposiciones del presente Reglamento, serán objeto del procesamiento que corresponda en el marco de la responsabilidad por la función pública, prevista en la Ley de Administración y Control Gubernamental Nº 1178 (SAFCO).*

..... o .....

ANEXO

GESTIÓN - 2009

ANEXO 1

ADQUISICIÓN, RENOVACIÓN Y BAJA DE EQUIPOS, IMPRESORAS Y ACCESORIOS DE COMPUTACIÓN

I. ENCARGADOS DE LA ADQUISICIÓN, RENOVACION Y BAJA DE EQUIPOS, IMPRESORAS Y ACCESORIOS DE COMPUTACION

El Departamento de Tecnología de Información, será el encargado de controlar, supervisar y autorizar la Adquisición, Renovación y Baja de Servidores, Equipos de Computación (PC de Escritorio, Portátil), Impresoras Laser, Escáner, Proyectores Multimedia y todo Accesorio de Computación solicitados por todas las unidades de trabajo dependientes del Gobierno Municipal de Santa Cruz de la Sierra.

II. PROCEDIMIENTO PARA ADQUISICIÓN DE EQUIPOS, IMPRESORAS Y ACCESORIOS DE COMPUTACIÓN

Cada unidad de trabajo dependiente del Gobierno Municipal de Santa Cruz de la Sierra, deberá enviar una comunicación escrita al Jefe del Departamento de Tecnología de Información solicitando las Especificaciones Técnicas Exigidas para la Adquisición de Servidores, Equipos de Computación (PC de Escritorio, Portátil), Impresoras Laser, Escáner, Proyectores Multimedia y todo Accesorio de Computación, esto con el fin de mantener una misma plataforma computacional, evitando así equivocaciones para la Adquisición de Bienes y Servicios solicitados por cada unidad, además se debe justificar la necesidad de la compra.

La Unidad Solicitante, una vez reciba las especificaciones técnicas, debe proceder a la búsqueda de los requisitos exigidos para iniciar un proceso de compra en las Normas Básicas de Administración de Bienes y Servicios y Subsistema de Contrataciones, y Reglamento Específico de Contrataciones del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, para luego realizar la solicitud de aprobación vía la Oficialía Mayor que corresponda. Una vez aprobada la misma, el Departamento de Contrataciones o Adquisiciones correspondiente, solicitará al Jefe del Departamento de Tecnología de Información un Informe Técnico para verificar si las cotizaciones adquiridas CUMPLEN o NO con las especificaciones técnicas exigidas.

El Departamento de Tecnología de Información, emitirá un Informe Técnico al respecto, indicando si procede o no la solicitud de compra, además se notificara los motivos y/o observaciones de adicción, modificación o cambio respectivo a la unidad solicitante si corresponden.

El Departamento de Adquisiciones o Contrataciones, una vez reciba toda la documentación correcta y aprobada para la adquisición de bienes o servicios; la Unidad Solicitante, procederá a seguir con el tramite respectivo para dicho proceso de compra.

Entre los puntos más importantes de las especificaciones técnicas exigidas por el Departamento de Tecnología tenemos que los Equipos de Computación (PC de Escritorio, Portátil) deben ser de MARCA RECONOCIDA (no se aceptarán equipos ensamblados más conocidos como chancho) y las Impresoras deben ser de tipo Laser tanto en Blanco/Negro o de Color; ambos ítems con 1 año de garantía de fábrica. El Departamento de Tecnología de Información, no dará curso a solicitudes de compra que no cumplan con las especificaciones técnicas exigidas.

III. PROCEDIMIENTO PARA RENOVACIÓN DE EQUIPOS, IMPRESORAS Y ACCESORIOS DE COMPUTACIÓN

Cada unidad de trabajo dependiente del Gobierno Municipal de Santa Cruz de la Sierra deberá enviar una comunicación escrita al Oficialía Mayor que corresponda solicitando autorización para la Renovación de Servidores, Equipos de Computación (PC de Escritorio, Portátil), Impresoras Laser, Escáner, Proyectores Multimedia y todo Accesorio de Computación con su debida justificación de la misma.

La Oficialía Mayor correspondiente, solicitará un Informe Técnico al Departamento de Tecnología de Información acerca de los Bienes y/o Servicios solicitados por la unidad a ser renovados. El Personal Técnico del Departamento de Tecnología, procederá a la revisión de los bienes solicitados para luego emitir un informe a su inmediato superior, y este a su vez ser enviado a Oficialía Mayor para fines consiguientes.

La Unidad Solicitante, una vez reciba la aprobación de Oficialía Mayor para renovación de Bienes y/o Servicios, debe iniciar y colocar en marcha el procedimiento para adquisición de equipos, impresoras y accesorios de computación de acuerdo a las normas de contratación establecidas y vigentes.

IV. PROCEDIMIENTO PARA BAJA DE EQUIPOS, IMPRESORAS Y ACCESORIOS DE COMPUTACIÓN

Cada Unidad de trabajo dependiente del Gobierno Municipal de Santa Cruz de la Sierra deberá enviar una comunicación escrita al Departamento de Bienes Patrimoniales vía la Oficialía Mayor que corresponda solicitando autorización para la baja de Servidores, Equipos de Computación (PC de Escritorio, Portátil), Impresoras Laser, Escáner, Proyectores Multimedia y todo Accesorio de Computación con su debida justificación de la misma.

El Departamento de Bienes Patrimoniales solicitará, solo si corresponde, un Informe Técnico al Departamento de Tecnología de Información acerca de los Bienes y/o Servicios solicitados por la unidad para que puedan darse de baja. Si corresponde, el Personal Técnico del Departamento de Tecnología de Información, procederá a la revisión de los bienes solicitados para luego emitir un informe a su Inmediato Superior, y este a su vez ser enviado al Departamento de Bienes Patrimoniales para fines consiguientes.

Cada funcionario es responsable de verificar en coordinación con el Departamento de Bienes Patrimoniales que todos los bienes o activos a darse de baja sean liberados de su poder mediante el llenado del formulario de Transferencia de Activos Fijos.

La Unidad Solicitante, una vez haya finalizado el proceso para baja de activos fijos, si desea iniciar un nuevo proceso de compra debe poner en marcha el procedimiento para adquisición de equipos, impresoras y accesorios de computación, de acuerdo a las normas básicas establecidas y vigentes de contrataciones y reglamentos específicos del Gobierno Municipal Autónomo de Santa Cruz de la Sierra.

Los Funcionarios Municipales del Gobierno Municipal Autónomo de Santa Cruz de la Sierra, que incumplan las disposiciones del presente Reglamento, serán objeto del procesamiento que corresponda en el marco de la responsabilidad por la función pública, prevista en la Ley de Administración y Control Gubernamental Nº 1178 (SAFCO) y el Reglamento de la Responsabilidad por la Función Pública, aprobado mediante Decreto Supremo N° 23318-A.

..... o .....