

MANUAL DE POLITICAS PARA LA SEGURIDAD INFORMATICA DE LA CONTRALORIA MUNICIPAL DE IBAGUE

TABLA DE CONTENIDO

INTRODUCCION	
1. OBJETIVO GENERAL	4
2. POLITICAS GENERALES	5
2.1. ACCESO A LA INFORMACIÓN	5
2.2. ADMINISTRACIÓN DE CAMBIOS	5
2.3. SEGURIDAD DE LA INFORMACION	5
2.4. SEGURIDAD PARA LOS SERVICIOS INFORMATICOS	6
2.5. SEGURIDAD EN RECURSOS INFORMATICOS	7
2.6. SEGURIDAD EN COMUNICACIONES	8
2.7. SEGURIDAD PARA USUARIOS TERCEROS	8
2.8. SOFTWARE UTILIZADO	9
2.9. ACTUALIZACION DE HARDWARE	9
2.10. ALMACENAMIENTO Y RESPALDO	10
2.11. CONTINGENCIA	10
2.12. AUDITORIA	10
2.13. SEGURIDAD FISICA	11
2.14. ESCRITORIOS Y COMPUTADORES LIMPIOS	11
2.15. ADMINISTRACIÓN DE LA SEGURIDAD	12
2.16. GENERALES	12
3. RECURSO TECNOLOGICO	14
3.1. HARDWARE	14
3.2. SOFTWARE	19
3.3. OTROS	20
4. USO DE INTERNET	21
5. SEGURIDAD Y CONTROL	23
6. PROTECCIÓN CONTRA VIRUS	24
7. GENERALIDADES	25
7.1. OPERACIONES BASICAS	25
7.2. IMAGEN INSTITUCIONAL	25
7.3. SEGURIDAD PERSONAL	25
7.4. SEGURIDAD FISICA	27
8. RESPONSABILIDADES	29
GLOSARIO	30

INTRODUCCIÓN

Hoy es imposible hablar de un sistema cien por ciento seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio e información o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar una suma considerable de dinero en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar mucho dinero".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas entidades gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), definidas en este documento para la Contraloría Municipal de Ibagué, surgen como una herramienta organizacional para concientizar a cada uno de los funcionarios de la entienda, sobre la importancia y sensibilidad de la información y servicios críticos.

1. OBJETIVOS

- 1.1. Establecer los lineamientos básicos que permitan mantener en óptimas condiciones de funcionamiento los recursos de Ti (tecnología informática: equipos de computo, software, información, entre otros) asegurando el control y seguridad de la información.
- 1.2. Controlar y soportar los recursos de datos de cómputo, software y hardware en la Entidad, buscando una adecuada administración ante las amenazas técnicas, físicas, tecnológicas y de inoperancia que las afecta.

2. POLÍTICAS GENERALES

Las políticas definidas en el presente documento aplican a todos los funcionarios públicos, contratistas y pasantes personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la CONTRALORIA MUNICIPAL DE IBAGUE.

2.1. ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas y pasantes que laboran para la CONTRALORIA MUNICIPAL DE IBAGUE deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la CONTRALORIA MUNICIPAL DE IBAGUE, es responsabilidad del cuerpo directivo, autorizar el acceso sólo indispensable a la información y a los equipos de cómputo, de acuerdo con el trabajo realizado por estas personas, previa justificación.

Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad. Terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

2.2. ADMINISTRACION DE CAMBIOS

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

2.3. SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas y pasantes de la CONTRALORIA MUNICIPAL DE IBAGUE son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, contratistas y pasantes de la CONTRALORIA MUNICIPAL DE IBAGUE deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información esta en la obligación de reportar el hecho al grupo de control interno disciplinario.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

Con respecto a la información contenida en la página WEB de la Entidad – www.contraloriaibague.gov.co – esta será publicada con autorización del Jefe encargado del área respectiva y bajo ningún otro criterio.

2.4. SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

El sistema de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes. Queda **prohibido la descarga** de archivos que no correspondan al trabajo realizado por cada funcionario, contratista o pasante.

En cuanto a los grupos de charla (Chat) y utilidades asociadas, **queda prohibido su uso**, excepto cuando el trabajo realizado lo amerite y por ende será autorizado por el jefe de la dependencia.

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito.

Los funcionarios públicos, contratistas y pasantes no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Entidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los funcionarios públicos, contratistas y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente comunicarlo a la persona encargada para atender estos casos, no utilizar el computador y desconectarlo de la red.

2.5. SEGURIDAD EN RECURSOS INFORMATICOS

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas y pasantes de la CONTRALORIA MUNICIPAL DE IBAGUE son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a el.

Antes de que un nuevo sistema se desarrolle o se adquiera, los subdirectores, jefes de oficina, en conjunto con el funcionario encargado de asesorar la Entidad en temas de informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y

seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

2.6. SEGURIDAD EN COMUNICACIONES

Las direcciones internas (IP), topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser considerados y tratados como información confidencial y no pueden ser modificadas sin previa autorización de la persona encargada de administrar el recurso informático de la Entidad.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

Los computadores de la CONTRALORIA MUNICIPAL DE IBAGUE se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del área de seguridad informática y/o la oficina de informática.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada.

2.7. SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los Recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de CONTRALORIA MUNICIPAL DE IBAGUE para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por el funcionario delegado por el Secretario General de la CONTRALORIA MUNICIPAL DE IBAGUE.

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador.

Si se requiere un equipo con módem, este equipo no podrá en ningún momento estar conectado a la Red al mismo tiempo.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el Secretario General con el fin de no comprometer la seguridad de la información interna de la entidad.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad.

Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la entidad. La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la entidad.

2.8. SOFTWARE UTILIZADO

Todo software que utilice la CONTRALORIA MUNICIPAL DE IBAGUE será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Todo el software de manejo de datos que utilice la CONTRALORIA MUNICIPAL DE IBAGUE dentro de su infraestructura informática, deberá contar con las técnicas apropiadas para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de la CONTRALORIA MUNICIPAL DE IBAGUE.

Está **prohibido el uso de software ilegal** dentro de la CONTRALORIA MUNICIPAL DE IBAGUE, así mismo la descarga de software a través de Internet y su posterior instalación.

El funcionario encargado de administrar el recurso informático de la entidad, está autorizado para monitorear periódicamente los equipos y en los casos de encontrar software instalado no licenciado por la Entidad, llevar a cabo las acciones correctivas e informar al Secretario General las irregularidades encontradas.

2.9. ACTUALIZACION DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del Jefe a cargo del área involucrada.

2.10. ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de la CONTRALORIA MUNICIPAL DE IBAGUE deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Las copias de seguridad se realizarán de acuerdo con los procedimientos establecidos en el manual.

El Jefe del área dueña de la información, con la asesoría de la persona encargada de administrar la infraestructura computacional de la CONTRALORIA MUNICIPAL DE IBAGUE, definirán la estrategia a seguir para el respaldo de la información y siguiendo los lineamientos definidos en el Manual de Procesos y Procedimientos.

Los funcionarios públicos son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas.

2.11. CONTINGENCIA

La administración de la Entidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

2.12. AUDITORIA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoria.

Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

2.13. SEGURIDAD FISICA

Siempre que un trabajador se de cuenta que un visitante no autorizado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores, impresoras, portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva por el Secretario General.

Los equipos de microcomputadores (PCS, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los funcionarios públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, ventiladores y en general cualquier equipos que generen caídas de la energía.

Los particulares en general no están autorizados para utilizar los recursos informáticos de la entidad.

Con respecto a los familiares de los funcionarios públicos, está prohibido el uso de los equipos informáticos para uso personal, descargas de música, juegos y software variado que interrumpa el normal desempeño de las actividades de los funcionarios.

2.14. ESCRITORIOS Y COMPUTADORES LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, s, Memorias Flash (USB), disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Es responsabilidad de los funcionarios públicos, contratistas y pasantes de la CONTRALORIA MUNICIPAL DE IBAGUE, mantener en buen estado los equipos de cómputo asignados para el desempeño de las labores diarias, igualmente se recomienda no consumir alimentos y bebidas que accidentalmente puedan ser

derramadas sobre los computadores, periféricos, documentos y otros elementos, con el fin de evitar daños irreparables en los mismos.

2.15. ADMINISTRACION DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Secretario General de la Entidad.

Los funcionarios públicos, contratistas y pasantes de la CONTRALORIA MUNICIPAL DE IBAGUE que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la oficina informática.

Los funcionarios que realicen labores de administración del recurso informático de la Entidad, divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Contralor, los casos de incumplimiento con copia al Secretario General y al Jefe de la Oficina Asesora de Control Interno, para que estos tomen las medidas correctivas correspondientes.

2.16. GENERALES

- Todo lo no expresamente permitido está prohibido al funcionario público (Art. 6 CPN).
- Toda Información Contenida, Procesada o Generada en los equipos de cómputo es propiedad de la Contraloría Municipal de Ibagué
- El usuario es el UNICO responsable de la información contenida en el o los PC'S asignados para ello. El usuario deberá determinar el grado de importancia y el tiempo que se debe conservar la información que amerita copias de seguridad, entre esta información tenemos la siguiente: Hojas de Excel, Documentos tipo Word. Carpeta de correo personal, Manejo de contactos para correo, Software de carácter no institucional.

- Antes de realizar un backup verifique el tamaño de los documentos a copiar y compáralo con el del medio en donde va a almacenar la copia, con el fin de determinar cuántos medios necesitará para que la copia quede completa.
- Verifique que el medio en donde va a copiar esté en buenas condiciones físicas, por ejemplo que el cd o dvd no esté con rayones, o que el disquete esté en buen estado y se pueda leer. De esta manera, asegura que la información posteriormente pueda ser recuperada.
- No deje visible sus contraseñas de correo, red y archivos, por que pueden ser utilizadas por otras personas alterando o dañando su información.
- No permita que personal externo opere su información, tampoco comparta sus contraseñas.

3. RECURSO TECNOLÓGICO

3.1. HARDWARE

- El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Director del Área
- Cada equipo esta preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y / o lógico del mismo incluyendo sus periféricos.
- En caso de presentar una falla física o lógica se deberá notificar a la Dirección Administrativa y en el caso de ser requerido enviar el equipo para su revisión y / o reparación de acuerdo al procedimiento establecido.
- En ningún caso el usuario intentara reparar el equipo ó diagnosticar, únicamente informar de la posible falla.
- El usuario será el único responsable del equipo de cómputo.
- En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
- El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
- En caso de que el usuario no tenga conocimiento y / o experiencia, se notifica a la Dirección Administrativa para su correspondiente capacitación.
- En caso de presentar una falla física o lógica se deberá notificar a la Oficina de Sistemas.
- La solicitud del equipo de cómputo será responsabilidad de la dependencia interesada, bajo las características técnicas definidas por la Oficina de Sistemas e información a las áreas relacionadas con la asignación de los recursos.

- Toda recepción de equipo de cómputo por adquisición o donación se realizará a través de la Dirección Financiera.
- Por ningún motivo se deberá violar la etiqueta de control ya que cualquier daño o cambio al hardware será responsabilidad de la persona a quien este resguardado.
- Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo.
- Cada equipo esta identificado en la red con un nombre de acuerdo con la ubicación de las oficinas de la entidad, como se muestra a continuación:

RELACIÓN DE COMPUTADORES

No	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Nombre Equipo
1	PC Escritorio	HP COMPAQ DX2400 MT	323	Rafael Enrique Bernal Poveda	Despacho Contralor	OF323-10
2	PC Escritorio	COMPAQ Presario SR53251a	323	Sandra Ximena Llanos Acosta	Despacho Contralor	OF323-2
3	PC Escritorio	HP Compaq DC5800	323	Inírida Pérez	Dirección Administrativa	OF323-1
4	PC Escritorio	DELL Optiplex 745	322	Maria Margarita Lombana Nuñez	Jurídica	OF322-1
5	PC Escritorio	Clon	322	Maria Margarita Lombana Nuñez	Jurídica	Of322-2
6	Portátil	Portátil HP 550	322	Maria Margarita Lombana Nuñez	Jurídica	Of322-3
7	PC Escritorio	Clon	322	Maria Margarita Lombana Nuñez	Jurídica	OF322-4
8	PC Escritorio	COMPAQ Presario SR5017LA	320	Audidores	Control Fiscal	OF320-2
9	PC Escritorio	COMPAQ Presario SG33131a	320	Elizabeth Torres Gaitán	Control Fiscal	OF320-1
10	PC Escritorio	HP Compaq Presario SR1617LA	320	Wilmar Chacon	Control Fiscal	OF320-3
11	PC Escritorio	DELL Inspiron 530	319	Maria Cristina Rubio Marín	Dirección Financiera	OF319-1

No	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Nombre Equipo
12	PC Escritorio	HP Compaq DC5800	319	Julio Cesar Gutiérrez Barrios	Dirección Financiera	OF319-2
13	PC Escritorio	HP Compaq EVO 5500 d220 MT	319	Julio Cesar Gutiérrez Barrios	Dirección Financiera	OF319-3
14	PC Escritorio	HP Compaq EVO 5502 d220 MT	318	Edgar Orlando Ríos Enciso	Control Interno	OF318-2
15	PC Escritorio	COMPAQ Presario SG3309la	318	Edgar Orlando Ríos Enciso	Control Interno	OF318-1
16	PC Escritorio	Acer Altos	318	Edgar Orlando Ríos Enciso	Control Interno	OF318-3
17	PC Escritorio	COMPAQ Presario SR5325la	316	Maria Eugenia Muñoz Martínez	Responsabilidad Fiscal	OF316-1
18	PC Escritorio	COMPAQ Presario SR5325la	316	Diana Yaritza Cubillos Ramírez	Responsabilidad Fiscal	OF316-2
19	PC Escritorio	COMPAQ Presario SG3309la	316	Reinel Ríos García	Responsabilidad Fiscal	OF316-3
20	PC Escritorio	COMPAQ Presario 4700	316	Diana Yaritza Cubillos Ramírez	Responsabilidad Fiscal	OF316-4
21	PC Escritorio	Clon	316	Diana Yaritza Cubillos Ramírez	Responsabilidad Fiscal	Of316-6
22	Portátil	Portátil HP 550	316	Diana Yaritza Cubillos Ramírez	Responsabilidad Fiscal	Of316-7
23	Portátil	PC Smart	316	Diana Yaritza Cubillos Ramírez	Responsabilidad Fiscal	
24	PC Escritorio	HP Compaq EVO 5500 d220 MT	314	Gloria Inés Muñoz	Control Fiscal	OF314-1
25	PC Escritorio	HP Compaq EVO 5502 dx 2000 MT	314	Jose Roberto Vásquez	Control Fiscal	OF314-2
26	PC Escritorio	HP Compaq DC5800	314	Herman Augusto Ríos Parra	Control Fiscal	OF314-3
27	PC Escritorio	HP Compaq DC5800	314	Maria del Pilar Gómez Vélez	Control Fiscal	OF314-4
28	PC Escritorio	COMPAQ Presario SR5017LA	314	Carlos Alberto Galeano Beltrán	Control Fiscal	OF314-5
29	PC Escritorio	Clon	314	Jose Roberto Vásquez	Control Fiscal	Of314-10

No	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Nombre Equipo
30	PC Escritorio	COMPAQ Presario 4700	314	Jose Roberto Vásquez	Control Fiscal	Of314-11
31	PC Escritorio	HP Compaq Presario SR1617LA	314	Jose Roberto Vásquez	Control Fiscal	Of314-12
32	Portátil	Portátil Lenovo	314	Jose Roberto Vásquez	Control Fiscal	
33	Portátil	Portátil COMPAQ Presario C7571a	314	Jose Roberto Vásquez	Control Fiscal	Of314-9
34	Portátil	Portátil HP 550	314	Jose Roberto Vásquez	Control Fiscal	Of320-4
35	Portátil	Portátil HP 550	314	Jose Roberto Vásquez	Control Fiscal	Of314-13
36	Portátil	PC Smart	314	Jose Roberto Vásquez	Control Fiscal	Of314-7
37	Portátil	PC Smart	314	Jose Roberto Vásquez	Control Fiscal	
38	PC Escritorio	COMPAQ Presario SG33091a	312	Olga Leonor Lerma Palma	Planeación y Participación	OF312-1
39	PC Escritorio	Clon	312	Olga Leonor Lerma Palma	Planeación y Participación	OF312-2
40	PC Escritorio	HP Compaq DC5100	312	Olga Leonor Lerma Palma	Planeación y Participación	OF312-3
41	Portátil	Portátil Lenovo	312	Olga Leonor Lerma Palma	Planeación y Participación	OF312-5
42	Portátil	Portátil HP 550	312	Olga Leonor Lerma Palma	Planeación y Participación	Of312-6
43	Portátil	PC Smart	312	Olga Leonor Lerma Palma	Planeación y Participación	Of312-8
44	Portátil	Portátil Compaq TX2510us	312	Olga Leonor Lerma Palma	Planeación y Participación	Of312-7
45	Servidor	Servidor DELL PowerEDGE 2800	306	Jairo Enrique Guzmán Cortés	Sistemas	
46	Servidor	Clon Qbex	306	Jairo Enrique Guzmán Cortés	Sistemas	
47	PC Escritorio	DELL Optiplex 745	306	Jairo Enrique	Sistemas	OF306-1

No	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Nombre Equipo
Guzmán Cortés						
48	PC Escritorio	QBEX - Clon	306	Luisa Alexandra Villa Olaya	Control Fiscal	OF306-2
49	PC Escritorio	Clon	306	Jairo Enrique Guzmán Cortés	Sistemas	OF306-3
50	Portátil	Portátil Compaq CQ40-5051a	306	Jairo Enrique Guzmán Cortés	Sistemas	OF306-4
51	PC Escritorio	HP COMPAQ DX2400 MT	305	Ruth García Ocampo	Control Fiscal	OF305-1
52	PC Escritorio	Clon	305	Ruth García Ocampo	Control Fiscal	OF305-3
53	PC Escritorio	COMPAQ Presario SR5017LA	305	Carmen Soraya Ariza Suárez	Control Fiscal	OF305-2
54	PC Escritorio	HP Compaq EVO 5502 dx 2000 MT	304	Nancy Franco Rios	Dirección Administrativa	Of304-2
55	Portátil	Portátil Compaq CQ40-5051a	304	Nancy Franco Rios	Dirección Administrativa	OF304-1
56	PC Escritorio	Clon	304	Nancy Franco Rios	Dirección Administrativa	OF304-3

RELACION DE IMPRESORAS

No.	Propiedad	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Ubicación / Equipo
1	CMI	Inyección	Hp Desject D 1560	323	Sandra Ximena Llanos Acosta	Despacho del Contralor	Of323-2
2	CMI	Láser	Kyocera FS1300D	323	Inírida Pérez	Dirección Administrativa	Of323-1
3	CMI	Inyección	Lexmark Z22	323	Inírida Pérez	Dirección Administrativa	Of323-1
4	CMI	Matriz de Punto	Epson LX-300+	322	María Margarita Lombana Nuñez	Oficina Jurídica	Of322-3
5	CMI	Láser	Kyocera FS1300D	322	María Margarita Lombana Nuñez	Oficina Jurídica	Of322-1
6	CMI	Matriz de Punto	Epson LX-300+	322	María Margarita Lombana Nuñez	Oficina Jurídica	Of322-2
7	IBAL	Matriz de Punto	Epson LX-300+ II	320	Elizabeth Torres Gaitán	Control Fiscal	Of320-1

No.	Propiedad	Tipo	Marca	Of.	Operario y/o Responsable	Dependencia	Ubicación / Equipo
8	CMI	Matriz de Punto	Epson LX-300+ II	319	Julio Cesar Gutiérrez Barrios	Dirección Financiera	Of319-2
9	CMI	Láser	HP LaserJet P1005	319	Maria Cristina Rubio Marín	Dirección Financiera	Of319-1
10	CMI	Inyección	HP Deskjet 3535	318	Edgar Orlando Rios Enciso	Control Interno	Of318-1
11	CMI	Matriz de Punto	Epson LX-300+ II	316	Maria Eugenia Muñoz Martínez	Responsabilidad Fiscal	Of316-1
12	CMI	Láser	HP LaserJet P1006	316	Diana Yartiza Cubillos Ramirez	Responsabilidad Fiscal	Of316-2
13	CMI	Matriz de Punto	Epson Lx 300 +	316	Diana Yartiza Cubillos Ramirez	Responsabilidad Fiscal	Of316-3
14	AGR	Láser	Kyocera FS1030D	314	Jose Roberto Vásquez	Control Fiscal	Of314-10
15	IBAL	Matriz de Punto	Epson LX-300+ II	314	Gloria Inés Muñoz	Control Fiscal	Of314-1
16	CMI	Matriz de Punto	Epson LX-300+	314	Maria del Pila Gómez Vélez	Control Fiscal	Of314-3
17	CMI	Inyección	HP DeskJet D1460	312	Olga Leonor Lerma Palma	Planeación y Participación	Of312-1
18	CMI	Matriz de Punto	Epson LX-300+	312	Olga Leonor Lerma Palma	Planeación y Participación	Of312-2
19	CMI	Inyección Multifuncional	HP DeskJet F4280	306	Jairo Enrique Guzmán Cortés	Sistemas	Of306-1
20	CMI	Matriz de Punto	Epson LX-300+ II	306	Luisa Alexandra Villa Olaya	Control Fiscal	Of306-2
21	CMI	Matriz de Punto	Epson LX-300+ II	305	Jose Roberto Vásquez	Control Fiscal	Of314-1
22	CMI	Inyección	HP DeskJet D1560	304	Nancy Franco Rios	Dirección Administrativa	Of304-2

3.2. SOFTWARE

- No deberá ser alterado
- Por ningún motivo el usuario instalará o descargará de Internet software de promoción y / o entretenimiento.
- El software no puede ser utilizado por el usuario para realizar trabajos personales.
- La adquisición o desarrollo de software será responsabilidad del área de informática.
- El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo de los programas básicos de operación de pc-s, siendo estos:

Sistema Operativo

- Windows xp
- Windows vista

Programas Ofimáticas

- Office 2007
- Open Office

Antivirus

- Nod 32: Actualizable automáticamente a través de Internet.

Otros

- Winrar : Software para comprimir archivos
- Acrobat: Edición de archivos PDF.
- Spark: Sistema de mensajería instantánea.
- Debían: Firewall o cortafuegos de Internet.

3.3. OTROS

La Entidad cuenta actualmente con un circuito eléctrico regulado soportando en 3 UPS.S de 3 KUA cada una, y una UPS de 600 VA que soporta el medidor de Internet.

Igualmente se cuenta con un sistema de cableado estructurado interconectado a través de 4 switan ubicados estratégicamente en 4 sitios de la entidad haciendo Back bonc instalados en jurídica, sistemas, Responsabilidad Fiscal y Participación Ciudadana. Estos rack se encuentran protegidos con sus respectivos gabinetes.

4. USO DE INTERNET

Internet trae grandes ventajas pero también puede ser un peligro para la entidad y la estabilidad laboral de los funcionarios. El abuso desmesurado, exagerado y sin consideración de parte de algunos funcionarios en detrimento del interés económico de las entidades es una de las desventajas más evidentes de Internet.

Una persona conectada todo el día a sitios como Messenger –MSN- en el cual puede dialogar horas y horas con sus amigos que al igual que él, también están conectados, termina “trabajando por ratos”, situación que no comprenden algunos funcionarios desconsiderados.

Por eso es que vemos muchas personas alcanzadas de tiempo y corriendo el viernes o sábado y el fin de mes, completando informes y demás.

Todos debemos plantearnos el siguiente interrogante: ¿Qué recursos de la oficina utilizo para mis actividades personales? Hace una década, la respuesta a este interrogante incluiría elementos como el teléfono, la impresora o el fax, entre otros. No obstante, el panorama cambió con la incursión de nuevas tecnologías de la información en el ámbito laboral.

Hoy en día, el 51% de las personas que laboran en entidades públicas y privadas navega en Internet entre una y cinco horas por razones personales, de acuerdo con los resultados de un estudio titulado Web@work, realizado anualmente por las compañías especializadas en el tema.

Leer correos electrónicos personales, descargar música o videos y realizar compras en línea son tareas que normalmente no están incluidas en las funciones de un cargo. Sin embargo, hasta qué punto estos hábitos afectan el desempeño laboral.

En términos generales debemos tener en cuenta que existen una serie de riesgos latentes con el uso de Internet en las organizaciones, considerando que tal vez usted aproveche la conexión de la entidad para tareas que requieren de un ancho de banda considerable.

En este sentido descargar videos y programas, escuchar emisoras en vivo o jugar en línea pueden parecer actividades inofensivas. No obstante, los resultados de Web@work concluyen que este tipo de actividades ocasionaron los problemas de red más comunes para las entidades durante el último año.

La instalación de software sin licencia o desautorizado por parte de los funcionarios también generó dolores de cabeza en las entidades. De otro lado, la encuesta estima que el 10 por ciento de las llamadas al servicio de soporte técnico prestado al interior de cada entidad, se originó por tareas no laborales que generaron conflictos. Además calcula que archivos personales como fotos,

videos o música ocupan la décima parte de la capacidad total de almacenamiento que tienen las entidades en discos duros.

En conclusión el uso de Internet está limitado por las políticas de seguridad de la Oficina de Sistemas. De otro lado, los Accesos a la red y a Internet serán solo de interés laboral y no personal. El usuario no deberá (ó copiar) archivos de la red sin autorización de la Oficina de Sistemas. Y al enviar información el responsable será el usuario correspondiente.

De ninguna manera se podrá acceder a páginas de entretenimiento, pornográfico o fuera del contexto laboral.

En caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará a la Oficina de sistemas, para analizar y evitar que ingresen virus al sistema.

5. SEGURIDAD Y CONTROL

- El área de sistemas auditará de manera periódica los equipos de cómputo y periféricos así como el software instalado.
- Cualquier salida y / o entrada de información tendrá que ser bajo la responsabilidad del jefe inmediato.
- Al usuario que requiera información deberá registrarse otorgando los datos para el control de entradas y salidas.
- Por ningún motivo deberán usarse equipos que no sean propiedad de la Contraloría Municipal de Ibagué
- En caso de que el usuario utilice un equipo que no sea propiedad de la Contraloría Municipal de Ibagué deberá notificar a la oficina de sistemas y el responsable de la dependencia deberá contar con la autorización de la Dirección Administrativa para su ingreso a la Entidad.
- Todos los equipos permanecerán en el lugar registrado por la Dirección Financiera.
- Solo los equipos portátiles de propiedad de la Contraloría Municipal de Ibagué podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.
- Todo servidor publico es responsable de salvaguardar su información, y debe hacer copias de seguridad por lo menos una vez en el mes como se especifica en el SIG. El cual puede ser consultado a través de la Internet.
- Los contratistas deberán entregar copia de seguridad de la información producida en desarrollo de su objeto contractual, como requisito para la liquidación de su contrato.
- Los interventores son responsables de verificar los medios magnéticos que reciben como producto o respaldo de objeto contractual.

6. PROTECCIÓN CONTRA VIRUS

El virus por computador puede definirse como un: “programa con capacidad de reproducir un error (infección) e insertarlo en las áreas de datos, de programas y en otras del mismo sistema y alterar su normal funcionamiento”. Estos, atacan destruyendo la integridad de la información contenida en los medios de almacenamiento magnético llegando incluso a dañar parte físicas de la maquina.

Aunque existe software antivirus, lo primordial es prevenir el contagio mediante la adopción de una política de “sano” procesamiento que el usuario debe seguir:

- Utilizar únicamente software autorizado e instalado por la Oficina de Sistemas.
- No debe instalar en los computadores software “pirata” ni de “juegos” o buscadores tales como KAZAA, EMULE, EDONKEY entre otros.
- No debe instalar “vacunas” sin la autorización de la Oficina de Sistemas. Estas aunque parezca irónico, pueden estar infectadas y pueden interferir en el normal funcionamiento del software antivirus utilizado por el Ministerio del Interior y de Justicia.
- No participar en el reenvío de cadenas de correo electrónico ni archivos o remitentes desconocidos.

7. GENERALIDADES

7.1. OPERACIONES BÁSICAS

- Para encender el sistema de computo verifique que el monitor, CPU, Impresora y demás periféricos que estén debidamente instalados entre si y conectados a la corriente eléctrica.
- Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.
- Encienda la impresora, monitor, y demás periféricos que tenga instalados dejando al final el CPU.
- Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado (algunos equipos requieren que se mantenga presionado el botón unos segundos).
- Encender y apagar el sistema:
- Al inicio y fin de las actividades.
- En caso de tormentas eléctricas.
- Si se presentan fallas eléctricas.

7.2. IMAGEN INSTITUCIONAL

- Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- En el exterior de todos los equipos se respetara la imagen física de empaque.
- Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

7.3. SEGURIDAD PERSONAL

- Parpadee continuamente para evitar que las pupilas se sequen, especialmente si usa lentes de contacto.

- Cambie periódicamente la dirección de su mirada para descansar el nervio ocular.
- Realice constantemente ejercicios de visión periférica.
- Mantenga limpia la pantalla del monitor para facilitar la lectura y evitar reflejos.
- Regule la iluminación del área para evitar el reflejo de la luz sobre la pantalla.
- Emplee filtros que oscurecen el brillo de la pantalla y disminuye la disipación de rayos ultravioleta (de vidrio o plástico en vez de maya, ya que este tiende a recoger el polvo).
- Ajuste la brillantez de la pantalla.
- Ajuste la posición de la pantalla y las fuentes de iluminación (luz natural y eléctrica).
- Coloque el monitor y los documentos fuente de manera que ambos estén aproximadamente a la misma distancia de sus ojos.
- Informe a la Dirección Administrativa, de aquellos monitores con mala resolución o parpadeo.
- Si utiliza lentes que sean con un marco completo para leer a una distancia de 50 a 60 centímetros
- Coloque el monitor de manera que la parte superior de la pantalla esté debajo de su línea visual.
- La vista fatigada puede indicar un problema de vista relacionado con algo más que el monitor de computadora.
- En lo posible utilice descansen muñecas y descansa pies con el fin de evitar problemas de columna y túnel del Carpo

7.4. SEGURIDAD FISICA

- Las tomas de color naranja, corresponden a salidas de corriente regulada, en las cuales se debe conectar únicamente los equipos de cómputo, para lo cual no deben conectarse elementos diferentes como celulares, televisores, radios, ventiladores, entre otros.



- Los patch cord ó cables que conectan cada equipo a la red de datos, deben estar completamente libres de obstáculos y no deben estar dispersos en el piso lo que ocasionaría que estén expuestos a que sean presionados por sillas, escritorios o por nosotros mismos al caminar sobre ellos.



- La canaleta debe estar totalmente tapada, sin tramos de cable a la vista. Al igual que los tramos de canaleta que contienen los tomacorrientes.



- El consumo de alimentos y bebidas sobre los equipos de cómputo, puede ocasionar daño en alguna de sus partes, o en el caso extremo algún corto circuito.



- Realizar el encendido y apagado correcto de los equipos de cómputo de acuerdo con la versión de Windows que tenga instalado.



- Cuando lo requiera y en especial al finalizar la jornada laboral, todos los equipos de cómputo deben quedar completamente apagados.



8. RESPONSABILIDADES

- Los responsables de cada área deberán apoyar al cumplimiento de los lineamientos antes mencionados.
- Todo usuario tendrá que cumplir con los lineamientos antes mencionados de lo contrario se hará acreedor a una sanción que se designara por el nivel directivo.
- Las medidas anteriores son enunciativas y no limitativas, el área de informática se mantendrá en contacto con los usuarios para hacerles saber de las nuevas disposiciones tecnológicas y de procedimiento.

GLOSARIO

Entiéndase para el presente documento los siguientes términos:

Política: Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la CONTRALORIA MUNICIPAL DE IBAGUE, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.

Ataque cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.

Criptografía de llave pública: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: Transformar un mensaje en un documento no legible, y el proceso contrario se llama "descodificar" o "descifrar". Los sistemas de ciframiento se llaman "sistemas criptográficos".

Certificado Digital: Bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Actualmente la Contraloría cuenta con un certificado digital emitido por Certicámaras, el cual es utilizado en algunos procesos de envío de información, en especial en el proceso de rendición de la cuenta a la Auditoría General de la República a través de su aplicativo SIREL.

No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.