0. JUSTIFICACION

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de la Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales y transgresores de la seguridad asociada a la información de misión crítica en las organizaciones.

Este riesgo inminente, obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar cualquier tipo de ataque, sabotaje, alteración o acceso no autorizado a la información, abarcando personas, datos, software, hardware, comunicaciones, instalaciones físicas y administración de seguridad.

El objetivo principal de la Oficina de Innovación y Tecnología de Comfatolima, es brindar a los usuarios los recursos informáticos con la calidad y cantidad que demandan, así como también preservar y mantener la información para que sea oportuna, confiable, entendible y relevante para la toma de decisiones.

1. INTRODUCCION

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han logrado gran auge, más aún con herramientas como el Internet y la tecnología Web, situación que ha conllevado la aparición de nuevas amenazas en los sistemas computarizados.

De esta manera, las políticas de seguridad de la información de Comfatolima, emergen como el instrumento para concienciar a sus funcionarios acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de fallas y de las debilidades, de tal forma que permitan a la entidad cumplir con su misión corporativa.

El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

2. ALCANCE

La presente política de seguridad de la información aplica para todos y cada uno de los funcionarios de Comfatolima que hagan uso de los equipos de cómputo de la Entidad, y/o que tengan acceso a información física que se considere confidencial o clasificada de igual forma a las terceras partes que se encuentren involucradas

3. POLITICAS

La oficina de IT de Comfatolima se encarga de brindar servicio directo al cliente interno, por el ámbito de competencia que tiene en materia de equipamiento, instalación, modificación, reparación, programación, etc. Por lo que ha sido necesario emitir políticas particulares para la infraestructura tecnológica y de manejo de información con que cuenta la Caja.

3.1 GESTION DE ACTIVOS

a) De la instalación de equipos de cómputo

i. Todo equipo de cómputo (computadores, impresoras, UPS, etc.) que posea Comfatolima, debe estar sujeto a las normas y procedimientos de instalación, operación, cuidado y mantenimiento que emite la Oficina de Innovación y Tecnología y adoptando las buenas prácticas (Procedimiento GIT-PR-015, GIT-PR-007).

ii. Las oficinas de IT y activos fijos, deberán tener un registro de todos los equipos de cómputo propiedad de Comfatolima (Procedimiento GIT-PR-001).

iii. Los equipos de cómputo que tengan misión crítica (ej. Servidores, computadores con información confidencial), deberán estar ubicados en áreas que cumplan con requerimientos de seguridad física, condiciones ambientales, alimentación eléctrica y las restricciones de acceso apropiadas para cada caso.

iv. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios se deben de

solicitar al área de Tecnología a través de la Intranet, opción requerimientos.

v. Los responsables de los equipos de cómputo en las áreas, deberán dar cumplimiento a los procedimientos establecidos para actualización, reubicación, reasignación y todo aquello que implique movimientos en su ubicación, adjudicación, misión, etc. Informando en cada caso a las Oficinas de Innovación y Tecnología y Activos Fijos, para la correspondiente actualización de datos de los equipos (Procedimiento GIT-PR-001).

vi. Ningún funcionario debe conectar o desconectar periféricos o dispositivos a cualquier equipo de cómputo, sin la debida autorización o supervisión del área de Innovación y Tecnología.

vii. A la línea regulada no deben ir conectados estabilizadores o reguladores de voltaje, estos equipos se deben conectar mediante multitoma.

viii. Los cables de energía y comunicaciones deben estar protegidos por canaletas u otro medio que impida interceptaciones o daños.

ix. A la corriente regulada no se deben conectar equipos diferentes a los informáticos como aspiradoras, brilladoras, ventiladores, radios, grabadoras, etc., puesto que en casos de fallas de energía éstos pueden consumir toda la carga disponible por la UPS y no permitir el proceso normal de almacenar la información al presentarse fallas eléctricas por periodos cortos.

x. Los colaboradores de ComfaTolima, deben reducir el riesgo de daño o perjuicio causado en equipos de cómputo por acciones inadecuadas (consumo de alimentos y/o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros).

xi. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de ComfaTolima, y que no son de su propiedad, serán responsabilidad única y exclusiva de sus dueños. ComfaTolima, no será responsable sobre estos equipos bajo ningún caso.

xii. Todos los colaboradores y usuarios externos deben devolver todos los activos de ComfaTolima que se encuentren a su cargo, al terminar

contrato o labor, de acuerdo a los procedimientos vigentes del área de Activos fijos y almacén.

xiii. La instalación de equipos ajenos a la Caja debe ser autorizada por el jefe de IT, debe ser solicitado a través de la opción de requerimientos dispuesto en la intranet, especificando el motivo por el cual se solicita, para todos los casos la configuración de acceso al servidor corporativo está prohibido en equipos que no sean propiedad de la Caja, pues la Caja deberá brindar las herramientas necesarias para la realización de las funciones de todos los empleados.

b) Del mantenimiento de equipos de cómputo

i. A la Oficina de Innovación y Tecnología de Comfatolima, corresponde brindar soporte técnico en software y hardware a las áreas, efectuando las reparaciones que se encuentren dentro de sus posibilidades. A proveedores externos corresponde la realización del mantenimiento preventivo y correctivo de los equipos, atendiendo también las reparaciones que, por su complejidad, requieran de personal especializado (Procedimiento GIT-PR-015).

ii. Queda estrictamente prohibido que personal de Comfatolima que no pertenezca a la Oficina de Innovación y Tecnología o a proveedores externos autorizados, realice actividades de mantenimiento o alteración de la configuración de los equipos de cómputo, instalación de software, cambio de direcciones IP, mascaras de sub. Red, identificación del equipo en la red, formateo de discos, manipulación interna de impresoras y periféricos y otras actividades que puedan ocasionar perdida de la información o deterioro de los equipos.

iii. A todo equipo de cómputo, comunicaciones y demás equipos de soporte, debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja (Procedimiento GIT-PR-007).

c) De la actualización de equipos de cómputo

i. Todo equipo de cómputo (computadores portátiles, estaciones de trabajo, servidores y demás relacionados), y los de telecomunicaciones que sean

propiedad de Comfatolima, podrán ser actualizados en sus características de software y hardware si se requiere, procurando con esto mantener y mejorar su calidad y desempeño (Procedimiento GIT-PR-015).

d) De la reubicación de equipos de cómputo

i. La reubicación de los equipos de cómputo se realizará cumpliendo las normas y procedimientos establecidos para ello.

ii. Todo cambio tanto físico como de software que se realice a los equipos, deberá ser registrado en la ficha técnica correspondiente (Procedimiento GIT-PR-001).

iii. La reubicación de un equipo de cómputo se llevará a cabo bajo la autorización del responsable del mismo, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

e) Bajas de Equipos

i. Al momento de dar de baja un equipo el departamento de activos fijos deberá notificar al departamento de IT para que este emita el concepto técnico como lo estipula el procedimiento CO-PR-024, mediante el diligenciamiento del formato CO-FO-012.

ii. El departamento de Innovación y Tecnología al momento de certificar la baja de dicho activo en el caso de equipos de computo verificará los programas que éste tiene para hacer el respectivo traslado de licencias para ser reutilizadas en otros equipos (en los casos en que el tipo de licencia lo permita), en el caso de partes que puedan ser reutilizadas en arreglos de otros equipos deberá levantar acta de las partes que se reutilizaran e inventariarlas.

iii. Para los equipos que se den de baja, se deberá conservar el número de licencia (Producto key) o (Service Tag y Code Express) para una posterior instalación del mismo y se debe eliminar del computador el sticker que contiene el numero de licencia (en los casos en que el tipo de licencia lo permita).

f. Préstamos y/o salidas de Equipos de Cómputo.

i. El préstamo o salida de los equipos de cómputo de las instalaciones físicas de Comfatolima, deberá ser notificado al área de Activos fijos con el fin de que se activen las respectivas pólizas en casos de perdida y/o daños, esto debe ser diligenciado por el jefe del área respectiva que solicite la salida de dicho equipo y deberá ser notificado al área de IT, para que registre en la ficha del equipo la salida del mismo.

ii. Cuando necesite acceder a internet deberá hacerlo desde redes privadas nunca desde zonas públicas.

iii. En el caso de requerirse accesos remotos deberá tenerse en cuenta lo contemplado en el apartado 3.2 Control de accesos encisos d y e.

iv. En el caso de robo o pérdida el funcionario deberá informar de inmediato a su superior, al área de activos y al área de IT para que esta proceda a eliminar accesos remotos si los hubiera y bloquee accesos que puedan permitir la fuga de información.

v. Para el caso de salida y/o traslados de equipos de misión crítica como es el caso de servidores, esto deberá ser autorizado por el Jefe del área de IT a través de un correo, una intranet o un oficio, quien a su vez deberá dar la autorización por cualquiera de estos medios en el cual se debe especificar el motivo de la salida y/o traslado, el jefe de IT o quien este designe, deberá coordinar personalmente el traslado de dicho equipo suministrando el medio de transporte optimo y seguro para estos casos, de igual forma se debe notificar al área de Activos Fijos para activar las pólizas.

3.2 CONTROL DE ACCESOS

a) Del acceso a áreas criticas

i. El acceso a los servidores centrales, Datacenter será permitido exclusivamente a los funcionarios de la Oficina de Innovación y Tecnología y/o a quienes sean autorizados por esta o por la Dirección General, o la secretaria general o la Subdirección Administrativa y Financiera.

ii. La Dirección General proveerá la infraestructura de seguridad requerida con base en los requerimientos específicos solicitados por el área de IT.

iii. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso al área de servidores estará sujeto a autorización de la Dirección General.

iv. Como mecanismo de prevención, todos los empleados y visitantes no deben comer, fumar o beber en la sala de servidores.

v. El acceso a los cuartos de comunicaciones ubicados en la sede administrativa y/o otras sedes de la caja será permitido exclusivamente a los funcionarios de la Oficina de Innovación y Tecnología y a quienes sean autorizados por ésta, por la Dirección General, secretaria general o por la Subdirección Administrativa y Financiera.

vi. Todo acceso a las áreas críticas deberá contar con un registro donde se especifique fecha, hora, labor a realizar, nombre del funcionario(s), área a la que pertenece, en caso de particulares deberán dejar también el registro con sus nombres, numero de documento de identidad, empresa a la que pertenece y un numero de contacto.

vii. El acceso a las áreas críticas debe ser restringido, el manejo de las llaves de acceso estará a cargo del área de IT, debe contarse con cámaras de seguridad, y sensores que se consideren necesarios con el fin de garantizar la seguridad y la continuidad del servicio.

b) Del control de acceso al equipo de cómputo

i. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos (Reglamento interno de trabajo Comfatolima, Capitulo XV, Artículo 56, enciso K).

ii. Las áreas donde se tengan equipos de misión crítica (servidores), estarán Sujetas a los requerimientos que la Oficina de Innovación y Tecnología emita.

iii. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Oficina de Innovación y Tecnología tiene la facultad de acceder a cualquier equipo de cómputo de la caja que no esté bajo su supervisión, además de realizar copias de seguridad de la información del equipo si lo considera conveniente y no es necesario que el funcionario responsable de dicho equipo de su autorización.

c) Del control de acceso local a la red

i. La Oficina de Innovación y tecnología es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, mediante la configuración del computador para que ingrese a la red, la asignación de los usuarios y claves de acceso requeridos para esto.

ii. Toda actividad informática no autorizada y/o controlada por el área de IT (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) que afecte tanto las redes como los sistemas de información de ComfaTolima, debe ser catalogada como ilícita y se podrá iniciar los procesos disciplinarios o legales a que haya a lugar.

iii. La Oficina de Innovación y Tecnología está facultada para dar seguimiento al uso de la red por parte de los usuarios.

d) Del control de acceso remoto

i. La Oficina de Innovación y Tecnología es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

ii. Para el caso especial de acceso a los servidores en entornos de administradores y/o desarrollo, esto deberá estar autorizado por el jefe del área de IT y deberá ser registrado en el GLPI.

iii. El área de IT deberá actualizar en el GLPI el registro de todos los accesos remotos, donde se especificará las razones por las cuales el funcionario dispondrá de acceso remoto en el equipo asignado y las observaciones que considere pertinentes, se deberá dejar registro del funcionario que realizo la configuración, este a su vez deberá constatar que una vez se conecte el funcionario no se pueda acceder a opciones críticas y será registrado en el GLPI en las observaciones del equipo.

iv. Los accesos remotos se deben realizar en equipos pertenecientes a la caja, se debe evitar al máximo realizar este tipo de instalaciones sobre equipos propiedad de los funcionarios de la caja y/o terceros los cuales se

harán solo por fuerza mayor y/o caso fortuito, en todos los casos éste accesos deberá estar autorizado por el jefe del área de IT.

v. En caso de detectar, percibir o sospechar acerca de un acceso no autorizado a la red desde el exterior, a través de enrutamientos ilegales, fallas en la seguridad, uso de contraseñas no autorizadas u otros mecanismos, la oficina de Innovación y Tecnología está autorizada para desconectar inmediatamente las conexiones hacia el exterior y si es el caso, suspender la prestación del servicio hasta que se neutralice la situación, se deberá dar aviso al Director General, o secretaria general, o Subdirector que se encuentre disponible en el momento.

vi. Todo acceso no autorizado que se registre en la red deberá ser documentado como un incidente en el GLPI.

vi. Todo dispositivo que permita realizar conexiones inalámbricas a la red corporativa de la Caja, debe estar configurado para impedir conexiones anónimas o no autorizadas al sistema.

e) De acceso a los sistemas de información corporativos

i. Tendrán acceso a los sistemas de información corporativos solo los funcionarios de Comfatolima y aquellos terceros que estén debidamente autorizados por el jefe del área de IT.

ii. El acceso a cada sistema de información corporativa (ej. Subsidio, contabilidad, nomina, etc.), será determinado por el jefe de cada área, especificando a su vez el usuario autorizado, las aplicaciones a las que tendrá acceso y los permisos de operación en cada aplicación (Procedimiento GIT-PR-006).

iii. El nombre de usuario y la clave de acceso a los sistemas de información corporativa, serán responsabilidad directa de cada funcionario, en lo referente al cambio periódico de claves, confidencialidad y uso personal e intransferible de los mismos y buenos usos de la información corporativa.

iv. Los usuarios deben cambiar sus claves de acceso máximo cada cuatro meses. Es recomendable que las claves contengan mínimo

ocho (8) caracteres y que estén compuestas por letras y números. (Ver numeral política de creación de claves).

v. En caso de vandalismo, daños intencionados o no a la información y otras anomalías ocasionadas manualmente, será responsable el funcionario dueño del nombre de usuario y la clave asociados a la situación.

vi. Es responsabilidad de cada jefe de área, velar que los usuarios habilitados para el acceso al sistema de información corporativa, sean activados o inactivados de acuerdo al caso, cuando el funcionario responsable sea trasladado, se encuentre en vacaciones, se retire de la empresa, etc.) (Procedimiento GIT-PR-006).

vii. Los recursos disponibles a través de la red corporativa (Intranet, Isolución, aplicaciones corporativas), serán de uso exclusivo para asuntos relacionados con las actividades propias de la Caja, en ningún momento con fines personales o de terceros.

viii. Elementos como el Chat corporativo y el correo electrónico a través de la intranet, no deben ser utilizados por ningún motivo para fines personales.

f) Del acceso a internet

i. La Oficina de Innovación y Tecnología es la única responsable de instalar y administrar los servidores de Internet, así como de mantener un esquema efectivo de seguridad para accesos no autorizados desde el exterior y restringir el acceso a sitios no autorizados por parte de los usuarios en las diferentes áreas.

ii. La configuración de accesos a Internet para las áreas, deberán solicitarse por escrito a la Oficina de Innovación y Tecnología, especificando además las páginas que se requieren como herramienta para el desempeño de las labores cotidianas (Formato GIT-FO-024).

iii. Al funcionario del área de IT responsable de los servidores Web, corresponde la verificación de respaldo y protección adecuada de estos equipos (Procedimiento GIT-PR-004).

iv. El material que aparezca en la página Web de Comfatolima, deberá ser revisado previamente por la oficina de publicidad, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

v. La Oficina de Innovación y Tecnología tiene la facultad de llevar a cabo la revisión periódica de los accesos a los servicios de información, y conservar información del tráfico.

vi. Se prohíbe el uso de cuentas de correo personales. Para intercambiar información laboral los funcionarios deberán solicitar la creación de su respectiva cuenta corporativa. Igualmente, estas cuentas serán monitoreadas por parte del área de sistemas, para garantizar su correcto uso.

vii. Se prohíbe el uso de programas de mensajería instantánea, programas de descarga y otros que afecten la disponibilidad y seguridad de la red.

g) Del acceso a la disponibilidad de la red

i. En caso de fallos en el fluido eléctrico, la red corporativa deberá estar soportada por una unidad de suministro ininterrumpido de poder (UPS) y a un nivel superior por una planta generadora de energía.

ii. Al momento de presentarse el fallo del suministro eléctrico, la autonomía de la red será asumida por la UPS, mientras que la planta generadora de energía se activa y asume la carga de la red.

iii. En caso de no contar con planta generadora de energía, al momento de presentarse la interrupción del fluido eléctrico, todos los funcionarios de la Caja que se encuentren trabajando en los equipos de cómputo deberán apagarlos inmediatamente, esto aprovechando el margen de tiempo que provee la UPS para permitir la salida correcta de los sistemas de computo.

iv. El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único de conmutación que cause la caída de todos los servicios. Debe utilizarse topología estrella para los cableados de voz, datos, fluido eléctrico.

h) Del acceso al ftp o Transferencias de archivos

i. El acceso a ftp para extracción de archivos será restringido, el jefe de IT deberá realizar un análisis previo de las necesidades y determinará si es fundamental para el cumplimiento de las tareas del funcionario que lo solicita, para todos los casos se debe hacer la solicitud a través de requerimiento por la opción dispuesta en la intranet para ello.

ii. Los programadores deberán procurar guardar un log de los reportes que se generan, lo más detallado posible.

iii. El área de IT deberá ejercer control y vigilancia sobre los logs de transferencias de archivos, esto con el fin de determinar quiénes y que tipos de archivos transfieren los usuarios, en casos donde se encuentren extracciones de información que generen sospechas, deberá informarse al jefe de IT quien se encargará de adelantar la investigación respectiva y es quien determinará si se suspende el acceso al servicio FTP.

iv. En caso de encontrarse que algún funcionario está haciendo mal uso de la extracción de información se deberá dar aviso de inmediato a la Dirección Administrativa para que se inicien los procesos disciplinarios respectivos.

3.3. POLITICA DE CONTRASEÑAS SEGURAS

a) Conexión servidor aplicaciones corporativas

La conexión del usuario con el servidor de aplicaciones consta de un login y una contraseña, el login es asignado por el departamento de IT y estará conformado por el nombre+apellido en caso de haber coincidencias el login podrá ser el segundo_nombre+apellido de tal forma que no se repita, no se crearan login donde no se puedan identificar las usuarios como por ejemplo pasante1, cartera1, la contraseña debe ser creada por el usuario y solo lo puede realizar el mismo usuario quien deberá firmar el GIT-FO-024.

b) Sistemas corporativos

La conexión del usuario con los aplicativos puede constar del ingreso del número de su cédula o un nombre de usuario (opcional en algunos aplicativos) y una contraseña, dicha contraseña no puede ser

compartida con otros usuarios, esta contraseña deberá tener una longitud mínima de 8 caracteres, máxima 15 caracteres, contener al menos una letra mayúscula, al menos una letra minúscula, contener números y caracteres especiales como (* - + / _ -), estas contraseñas deberán ser cambiadas al menos cada 120 días, en caso de recuperación, se deberá hacer directamente por el funcionario, para ello deberá notificar al área de IT para que esta dependencia después de verificar que se trata del usuario proceda a resetear de nuevo la clave con el fin de que el usuario pueda ingresar una nueva clave.

c) Encriptación de claves

Las claves de acceso a los sistemas corporativos deberán contar con un proceso de encriptación, esto con el fin de no almacenar claves explicitas en las Bases de Datos.

d) Préstamo de usuarios y claves.

Queda prohibido el préstamo de usuarios y claves, se considera como una falta grave el incurrir en esta conducta y en caso de encontrarse esta situación se deberá levantar una violación diligenciando el formato GIT-FO-014, en los casos en que se presenten alteraciones indebidas de información el resultado de la auditoria en el sistema

3.4. GESTIÓN SOFTWARE

a) De la adquisición de software

i. Cuando un área de la Caja requiera el desarrollo de software deberá seguir el procedimiento GIT-PR-015, en caso de adquisición de una herramienta de software específica, deberá seguir el procedimiento GIT-PR-016.

ii. Todo programa de computo que se encuentre instalado en los equipos de computo, deberá contar con la licencia de adquisición del mismo, excepto en los casos de software libre distribuido por Internet o cedido por un tercero, caso en el cual deberá existir autorización escrita de uso por parte de la persona o entidad que cedió esta herramienta para uso por parte de Comfatolima.

iii. Programa de cómputo que se encuentre instalado sin autorización de la Oficina de Sistemas y en forma ilegal, será desmontado inmediatamente por dicha oficina.

iv. En caso de que un ente de vigilancia de derechos de autor en software, encuentre en un equipo software ilegal o no autorizado, será responsable y asumirá las consecuencias la persona que tenga dicho equipo asignado.

b) De la instalación de software

i. En los equipos de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

ii. La instalación de software que, a criterio de la Oficina de Innovación y Tecnología, pudiera poner en riesgo los recursos de la institución no está permitida.

iii. Con el propósito de proteger la integridad de los sistemas informáticos, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus y otros que se apliquen).

iv. Las áreas deberán informar a la Oficina de Innovación y Tecnología, cuando un equipo no tenga un antivirus o este se encuentre averiado o no este funcionando correctamente. En este caso la Oficina de Innovación y Tecnología tomará los correctivos necesarios.

v. La protección lógica de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier anomalía a la Oficina de Innovación y Tecnología.

c) De la actualización de software

i. Corresponde a la Oficina de Innovación y Tecnología autorizar cualquier adquisición y actualización del software.
ii. La oficina de IT deberá estar pendiente de la programación de las actualizaciones automáticas que se corren en cada equipo, las cuales deberán programarse en horarios que no interrumpan las labores de los funcionarios.

d) De la auditoria de software instalado

i. La Oficina de Innovación y Tecnología es responsable de realizar revisiones periódicas para asegurar que solo software con licencia esté instalado en los computadores de la Caja (Procedimiento GIT-PR-001).

ii. La oficina de IT en cualquier momento podrá realizar la revisión del software instalado en los equipos de la caja sin solicitar autorización del funcionario que tiene a su cargo el equipo de cómputo y en caso de encontrar software no autorizado deberá proceder a eliminarlo y dejar constancia en el formato GIT-FO-014.

e) Del software propiedad de la institución

i. Todo software adquirido por la Caja sea por compra, donación o cesión, es de propiedad de Comfatolima y mantendrá los derechos que la ley de propiedad intelectual le confiera.

ii. La Oficina de Innovación y Tecnología deberá tener un registro de todos los programas propiedad de la Caja.

iii. Todos los programas desarrollados por la Oficina de Innovación y Tecnología, se mantendrán como propiedad de Comfatolima.

iv. Es obligación de todos los usuarios del sistema informático, mantener el respaldo correspondiente de la información que reposa en sus discos duros, ya que se considera como un activo de la Caja que debe preservarse (Procedimiento GIT-PR-004).

v. Corresponde a la Oficina de Innovación y Tecnología efectuar copias de respaldo de la información corporativa (Procedimiento GIT-PR-004).

3.5 DE LA PREVENCIÓN CONTRA LOS VIRUS INFORMÁTICOS

Esta directiva aplica para todos los medios magnéticos (disquetes, memorias USB, CD's, DVD's y archivos descargados de Internet.

i. Verificar contra virus todos los medios magnéticos que se introduzcan en la computadora, aunque solo sean de datos.
ii. No ejecutar programas de origen dudoso.
iii. Nunca arrancar desde CD en la operación normal de la computadora.
iv. Nunca dejar en puestos CD, memorias, discos duros portátiles al apagar la computadora.
v. Los usuarios solo deben manejar medios magnéticos que contengan datos, los medios que contengan programas deben ser revisados previamente por la Oficina de Innovación y Tecnología.
vi. Los usuarios deben mantener copias de respaldo de sus datos.
vii. Se debe evitar abrir correos electrónicos de dudosa procedencia, cuando se tenga sospecha sobre estos correos se deberá consultar con el área de IT.

3.6 DE LA INFORMACION

a) De la confidencialidad

i. Todos los funcionarios de la Caja que tengan acceso a la información en medio lógico, magnético o físico, deberán cumplir los principios de reserva y confidencialidad especificados en el reglamento interno de trabajo (Reglamento interno de trabajo Comfatolima, Capitulo XV, Artículo 55, Numeral 2).

ii. Los funcionarios no deben suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas.

iii. Los funcionarios no deben destruir, copiar o distribuir los archivos de la entidad sin los permisos respectivos.

iv. Todo funcionario que utilice los recursos informáticos de la Caja, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada con crítica.

v. La información de la Caja no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de la entidad.

vi. Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la Caja. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

b) De la integridad

i) Para reducir la probabilidad de ingreso erróneo de datos a las aplicaciones corporativas, todos los formularios y procedimientos de ingreso de información deben contener controles de validación, tanto de tipo de dato como de nulidad y parametrización, siendo esto responsabilidad directa de los Analistas Programadores de la Oficina de Innovación y Tecnología.

ii) Por lo menos una vez al año los Analistas Programadores de Sistemas, deberán efectuar revisiones a los permisos de acceso a las aplicaciones en todos y cada uno de los usuarios registrados en el sistema, tanto a nivel de interfaz con el usuario (formularios), como de acceso a la Base de Datos a través del motor SQL, con esto se garantiza que los usuarios solo pueden acceder a datos autorizados para su cargo y efectuar solo las operaciones permitidas.

iii) Es responsabilidad directa de los Analistas Programadores, garantizar que todos y cada uno de los módulos de software de la Caja tengan un sistema de auditoria o registro de transacciones y operaciones registradas en el sistema, en el cual quede especificado fecha, hora, usuario, maquina, opción, operación y datos afectados.

c) Del respaldo físico

i. Diariamente, los Analistas Programadores y los Operadores de Sistemas deberán generar, verificar y almacenar copias de seguridad de toda la información corporativa, dando cumplimiento al procedimiento establecido para este fin (GIT-PR-004).
ii. Periódicamente, los usuarios finales deberán generar copia de seguridad de los datos que reposan en los computadores a su cargo, enviando esta copia a la oficina de sistemas para su control y custodia.

3.7. PLAN DE CONTINGENCIA - BCP

El plan de contingencias y recuperación general o plan de continuidad del Negocio (BCP) debe incluir un proceso estándar que integre los planes de contingencia para computadoras y comunicaciones, así como también el inventario de hardware y software existente. (Referirse al GIT-MA-001)

3.8. USO DEL CORREO ELECTRONICO

La información que repose en los equipos tecnológicos y en el correo electrónico pertenece a la caja, razón por lo cual se debe hacer buen uso de la misma, por ello queda prohibido:

- Utilizar el correo electrónico para finalidades privadas o personales;
- Utilizar el correo electrónico facilitado por COMFATOLIMA, para contratar servicios personales no relacionados con la actividad profesional o con las actividades propias del cargo;
- Usar programas de chat, acceso a redes sociales, uso mensajería instantánea u otras aplicaciones similares durante la jornada de trabajo, a menos que dichas redes o aplicaciones tengan relación con las funciones encomendadas.
- El acceso a cuentas de correos personales para uso laboral y personal.
- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en ComfaTolima, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el jefe de área.
- No se debe abrir correos de dudosa procedencia, en caso de tener dudas deberá comunicarse con el área de IT.
- El envió de correos electrónicos masivos a personas externas (15 En adelante), deberá hacerse mediante solicitud al área de IT a través de la intranet por la opción de requerimientos.
- Para el envío de correos electrónicos a menos de 15 destinatarios deberá hacer uso del correo corporativo, siempre utilizando la copia oculta CCO.
- Todas las cuentas de correo electrónico deben ser identificadas con la firma del responsable, siguiendo los lineamientos impartidos por el área de protección de Datos de la caja.

- Es responsabilidad de cada encargado del correo corporativo de su dependencia informar a su grupo de trabajo y al área de protección de datos personales los casos en que producto de una comunicación el destinatario manifieste que no desea recibir correos electrónicos y deberá eliminar de forma inmediata de su lista de contactos este destinatario.

3.9. USO CORREOS MASIVOS, MENSAJERIA INSTANTANEA.

- El uso de correos masivos estará restringido para cualquier funcionario de la caja, para ello el jefe del área respectiva deberá solicitar al área de IT el apoyo para el envió de esta información.
- En los casos en que producto de una comunicación el destinatario manifieste que no desea recibir correos electrónicos se deberá eliminar de forma inmediata de la lista de contactos este destinatario y se notificará al área de PDP de la Caja.

3.10. PROTECCIÓN DE DATOS PERSONALES

Para las directrices relacionadas con la protección de datos personales de COMFATOLIMA ver gestiones incidentes de seguridad en el tratamiento de datos personales (JU-MA-002)

4. Generalidades

- Comfatolima debe contar con un comité de seguridad, el cual estará conformado por el Director General o su representante, el jefe de la Oficina de la Secretaria General, el Subdirector Administrativo y Financiero, el Jefe Área SIG, y el jefe de la Oficina Innovación y Tecnología, quienes deberán tratar temas referentes al análisis y evaluación del SGSI y las directrices a tomar con respecto a este tema. Las reuniones de este comité serán solicitadas por la Oficina de Innovación y Tecnología cuando se consideren necesarias y como mínimo una vez por año.
- La Oficina de Innovación y Tecnología, como principal promotora del SGSI, deberá utilizar las herramientas que estén a su alcance con el fin de divulgarla, socializarla y sembrar conciencia en cada uno de los funcionarios de la caja.

- El manual de políticas de seguridad de la información rige a partir de su aprobación y publicación dentro de los documentos del SIG.
- Se efectuará seguimientos al cumplimento del presente manual, a través de la Lista de Chequeo Cumplimiento Política de Seguridad GIT-FO-026, la cual se aplicará a todos los puestos de trabajo mínimo una vez al año.

5. Sanciones

i. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento interno de trabajo, se conservará registro en el formato Violación Políticas de Seguridad (GIT-FO-014).

ii. Corresponderá a la Oficina de Innovación y Tecnología informar a la Dirección General sobre cualquier violación al presente manual, así mismo dicha dirección será la encargada de adelantar cualquier investigación o de delegar esta función a quien considere competente.

iii. Todas las acciones que comprometan la seguridad informática y que no estén previstas en esta política, deberán ser revisadas por la Dirección General, La Oficina Secretaria General y la Oficina de Innovación y Tecnología para emitir un veredicto.

6. Bibliografía

i. Política Oficial de Seguridad Informática del CICESE – México (http://telematica.cicese.mx/seguridad/poli-segu.pdf).

ii. Asobancaria – Políticas de seguridad informática del sector financiero colombiano (http://www.asobancaria.com/upload/docs/docPub2822_1.pdf).

7. GLOSARIO

i. IT: Oficina de Innovación y tecnología encargada de ofrecer sistemas de información integrales, permitiendo en forma oportuna satisfacer necesidades de información.

ii. Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

iii. Misión Crítica: Equipos o información que reviste gran importancia para el desarrollo de las funciones de una organización, en el caso de Comfatolima, los equipos de cómputo de misión crítica más relevantes son los servidores donde se encuentra almacenada la información de subsidio, contabilidad, tesorería, activos, nómina (entre otros).

iv. Control de Acceso: técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos. Es una característica física o lógica de un sistema de información para permitir o negar el uso de sus componentes o funciones.

v. SGSI: (Sistema Gestión Seguridad de la Información)

El sistema de seguridad de la información o **SGSI** (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa.

8. DOCUMENTOS Y REGISTROS REFERENCIADOS:

- GIT-PR-001 Realizar el inventario de hardware y software
- GIT -PR-004 Realización de Backups
- GIT -PR-006 Administración cuentas de usuarios
- GIT -PR-007 Mantenimiento preventivo equipos de computo
- GIT -PR-016 Adquisición de herramienta de software especifica
- CO-PR-024 Baja de activos o elementos inservibles
- CO-FO-012 Concepto Técnico

- Licencias
- Reglamento interno de trabajo (GH-RE-001)
- Violación Políticas de Seguridad (GIT -FO-014)
- Lista de Chequeo Cumplimiento Política de Seguridad GIT -FO-026
- Gestiones incidentes de seguridad en el tratamiento de datos personales (JU-MA-002).

9. IDENTIFICACIÓN DE CAMBIOS:

Versión	Fecha de aprobación	Descripción de cambios
01	27/11/2009	- Adición del Formato Violación Políticas de Seguridad (SI-FO-014). - Adición al numeral F de los incisos vi y vii.
02	26/04/2011	- Adición al numeral 3.2 el inciso v.
03	14/03/2012	- Adicionar Lista de Chequeo Cumplimiento Política de Seguridad SI-FO-026
04	06/12/2019	- Ajustes de cargos
05	18/07/2022	- Adicionar aspectos relacionados con el uso de los equipos de cómputo y la información.