1405 18 JUN. 2019

# CAMARA DE REPRESENTANTES

# MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA CAMARA DE REPRESENTANTES

2019

# TABLA DE CONTENIDO

1405 18 JUN. 2019

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA

CAMARA DE REPRESENTANTES

## 1. INTRODUCCION

La Cámara de Representantes estipula que la información es de gran importancia para la misma ya que de ella emanan las acciones misionales que le fueron encargadas por la constitución política y la ley, por tal motivo se generan medidas para su protección y confidencialidad.

La presente política de Seguridad de la Información debe ser adoptada por los todos los funcionarios (Planta, UTL) y contratistas y visitantes en las instalaciones de la Cámara de Representantes, este documento se encuentra enfocado en las buenas prácticas de seguridad de la información, la estrategia de Gobierno en Digital en los lineamientos de la norma técnica ISO 27001/2013.

## 1. OBJETIVOS

## 2. OBJETIVO GENERAL

Establecer las políticas y procedimientos relacionados con la seguridad y protección de la información de la CÁMARA DE REPRESENTANTES frente a peligros internos y externos. Alineados con el marco de direccionamiento estratégico y de gestión del riesgo, con el fin de asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

Las políticas, constituyen esencialmente, orientaciones, normas, procedimientos e instrucciones que indican cómo manejar los asuntos de seguridad informática. También incluye la forma de comprobar el cumplimiento de estas políticas, las faltas en que se incurren y las eventuales medidas/sanciones disciplinarias a ser aplicadas.

## 3.1. OBJETIVOS ESPECÍFICOS

La CÁMARA DE REPRESENTANTES para el cumplimiento de su misión, visión, objetivos estratégicos y valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

a) Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas o practicantes de la Entidad respecto al correcto manejo y protección de la información que es gestionada y resguardada en la CÁMARA DE REPRESENTANTES.
b) Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
c) Implementar el Sistema de Gestión de Seguridad de la Información.
d) Proteger la información y los activos tecnológicos de la Entidad.
e) Asegurar la identificación y gestión de los riegos a los cuales se exponen los activos de información.
f) Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.
g) Atender las necesidades para el cumplimiento de la función misional.
h) Proteger la información y los activos tecnológicos de la Entidad.
i) Concientizar a los funcionarios, contratistas y practicantes sobre el uso adecuado de los activos de información puestos a su disposición para la realización de sus funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información.
j) Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno Digital respecto a la Seguridad de la Información.

## 3. ALCANCE

La Política de Seguridad de la Información, aplica a toda la Corporación, sus funcionarios, proveedores, contratistas y practicantes que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Entidad.

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de la CÁMARA DE REPRESENTANTES, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido

el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La CÁMARA DE REPRESENTANTES, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Dar cumplimiento a la Ley 1712 de 2014 Ley de Transparencia y el Acceso a la Información Pública.
b) Transparentar los procesos misionales y administrativos de la Corporación.
c) Garantizar la transparencia, la protección y el acceso a la información.
d) Minimizar el riesgo de los procesos misionales de la Entidad.
e) Cumplir con los principios de seguridad de la información.
f) Cumplir con los principios de la función administrativa.
g) Mantener la confianza de los grupos de interés.
h) Apoyar la innovación tecnológica.
i) Implementar el sistema de gestión de seguridad de la información.
j) Proteger los activos de información.
k) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
l) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la CÁMARA DE REPRESENTANTES.
m) Garantizar la continuidad de la gestión frente a incidentes.

## 4. TERMINOS Y DEFINICIONES

**Datos:** Son atributos propios en este caso pertenecientes a la Cámara de Representantes.

**Aplicaciones:** Son todas aquellas soluciones informáticas para gestión de la información como; KACTUS Y SEVEN.

**Servicios:** Son los prestados a la Cámara de Representantes como; Internet, IPTV (Servicio de Televisión), Telefonía.

**Equipo de Computo:** Son todos los equipos pertenecientes a la Cámara de Representantes para procesar la información.

**Internet:** Servicio prestado por la Cámara de Representantes a todos sus funcionarios para poder acceder a plataformas digitales.

**ISO 27001/2013:** Norma internacional emitida por la Organización Internacional de Normalización (**ISO**) y describe cómo gestionar la seguridad de la información en una empresa.

**SGSI:** Sistema De Gestión De Seguridad De La Información.

**Virus Informático:** Programa malicioso que se introduce en un equipo de cómputo, sin permiso o sin conocimiento de su usuario, para alterar su funcionamiento.

**PC:** Computador Personal.

**LAPTOP:** Computador Portátil.

**ROUTER:** Dispositivo de red que se encarga de llevar tráfico por la red.

## 5. ADMINISTRACIÓN DE HARDWARE Y SOFTWARE

Corresponde a la Oficina de Planeacion y Sistemas, proveer las especificaciones técnicas de cualquier equipo informático, la instalación de software y equipos computacionales, como también la realización de las pruebas técnicas respectivas.

Todo equipo de cómputo (impresora, scanner, monitor y otros recursos informáticos) perteneciente a la Cámara de Representantes, deberá permanecer en el lugar asignado por la Dirección Administrativa. El traslado o cambio de cualquier equipo debe ser autorizado por el Jefe de la Oficina de Planeación y Sistemas.

Luego de adquirido el activo informático le corresponde a la Oficina de Planeación y Sistemas de la Cámara de Representantes las siguientes responsabilidades:

a) Evaluar y aprobar el análisis de riesgos, planes de contingencia y prevención de desastres.
b) Implementar y velar por el cumplimento de las políticas, normas y procedimientos de seguridad Informática de toda la Cámara de Representantes.

c) Estandarizar la seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro, eficiente y eficaz.

d) Garantizar que exista en la entidad apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad informática y en particular en los casos de infección de virus, ataque de hackers, accesos no autorizados, fraudes y otros percances.

e) Establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

f) Elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática.

## 6. POLÍTICAS GENERALES DE SEGURIDAD TECNOLÓGICA DE LA CÁMARA DE REPRESENTANTES

La Oficina de Planeación y Sistemas ha establecido las Políticas de seguridad para los equipos de cómputo, accesorios y Software que se utilizan en para el funcionamiento de la entidad, buscando así la maximización de la estabilidad, consistencia y seguridad de los componentes informáticos de la entidad. Teniendo en cuenta lo anterior se detallan a continuación políticas que deben ser socializadas a todo el personal de planta y sus apoyos, por parte de la Dirección Administrativa. Las políticas son las siguientes:

a) Usar los computadores en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implementado las medidas de control apropiadas para proteger el software, el hardware y los datos. Estas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

b) Usar los equipos de cómputo para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

c) Respetar y no modificar la configuración de hardware y software establecida por la Oficina de Planeación y Sistemas atendiendo a las políticas establecidas en el presente Manual.

d) No manipular alimentos sobre los equipos computacionales teniendo especial cuidado de no derramar líquido en ellos.

e) Proteger los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

f) Toda falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o interrupción de los servicios.

g) Proteger los equipos para disminuir el riesgo de robo, destrucción, y mal uso.

h) No mover los equipos o reubicarlos sin autorización previa; para llevar un equipo fuera de la institución se requiere una autorización escrita del Jefe de Planeación y Sistemas; en el caso de los computadores portátiles bastará con la autorización del respectivo jefe inmediato de cada División o Sección.

i) Reportar inmediatamente a la Dirección Administrativa, pérdida o robo de cualquier componente de hardware o programa de software.

j) Para prevenir el acceso no autorizado, los equipos están configurados de manera tal que al cabo de diez (10) minutos de inactividad, se active el protector de pantalla y se bloquee el acceso al computador, por lo que se requiere ingresar nuevamente la contraseña para reanudar la actividad. El usuario debe bloquear su computador presionando las teclas CTrl + Alt + Supr ó Windows + L, cada vez que se ausente de su oficina.

k) El protector de pantalla y fondo de escritorio deben ser los institucionales. No se permite el uso de estos de manera personalizada tanto en los computadores de escritorio como en los portátiles que son propiedad de la Cámara de Representantes.

l) Los datos confidenciales que se muestran en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y del protector de pantalla.

m) En todas las aplicaciones desarrolladas, debe implementarse 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.

n) No está permitido el uso de módems en los computadores propiedad de la Cámara de Representantes.

o) 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 instalar software ilegal (Sin licencia), hacer copias o usar ese software tanto adquirido como desarrollado, para fines personales.

p) Los usuarios no deben copiar a un medio removible (como DVD, USB, CD, etc.), el software o los datos residentes en las computadoras de la Cámara de Representantes con el propósito de proporcionar información a personal ajeno a la Institución.

q) Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe desconectar de la red y notificar inmediatamente a la Oficina de Planeación y Sistemas, para que se tomen las acciones respectivas.

r) Debe utilizarse un programa antivirus para examinar todo archivo que venga de afuera o inclusive de manera interna. Este antivirus está instalado de forma predeterminada en cada uno de los

computadores de la Cámara de Representantes y administrado por la Oficina de Planeacion y Sistemas.

s) Queda prohibido bajar de Internet, software libre, gratis, demos, y en general software que provenga de una fuente distinta de Entidades Públicas Oficiales. La Dirección Administrativa o la Oficina de Planeación y Sistemas es la responsable de proveer el software de trabajo asignado a cada computador de acuerdo a la disponibilidad de licencias.

t) 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.

u) Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

v) Cada usuario es responsable de la información almacenada en su computador, por lo tanto, periódicamente debe hacer el respaldo de los datos guardados en PC´s y las copias deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones.

w) La información de la Cámara de Representantes es clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado y que hayan sido probadas y aprobadas por la Dirección Administrativa y la Oficina de Planeación y Sistemas.

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

y) Siempre que sea posible, deberá respaldarse y/o eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar.

z) El personal que está autorizado y utiliza un computador portátil que contenga información confidencial de la Institución, no debe dejarla desatendida, sobre todo cuando esté de viaje, además esa información debe estar cifrada.

aa) El espacio disponible en los discos duros es para almacenamiento de información relacionada con el trabajo.

## 7. POLÍTICAS PARA EL USO DE HARDWARE:

a) No deben abrir o romper los sellos de seguridad instalados en cada computador por la Dirección Administrativa y Oficina de Planeación y Sistemas.

b) No abrir, retirar o cambiar componentes de los equipos.

c) Evitar prestar e intercambiar los equipos computacionales.

d) Evitar instalar dispositivos o periféricos sin la supervisión y autorización expresa de la Oficina de Planeación y Sistemas.

e) No retirar o sacar equipo de la institución sin previa autorización del área de almacén.

## 8. POLÍTICAS PARA EL USO DE SOFTWARE:

a) El equipo que sea entregado al usuario contendrá en el disco duro el software básico, siendo estos los definidos por la Oficina de Planeación y Sistemas, como estándar para su operación y funcionamiento.

b) Cualquier otro software que requiera el usuario, deberá ser solicitado a la Oficina de Planeación y Sistemas, previo licenciamiento adquirido por la Cámara de Representantes.

c) La solicitud de algún Sistema o Software que se requiera debe ser enviada por escrito por el funcionario de la planta de personal con la necesidad de estos y con la debida justificación a la Oficina de Planeación y Sistemas, señalando los beneficios que tendría su obtención en la mejor realización de su trabajo. La Oficina de Planeación y Sistemas, analizadas las ventajas institucionales lo incluirá en su programa de adquisición o plan de adquisiciones.

d) El usuario deberá mantener los archivos de su equipo ordenados, siendo de su responsabilidad conservar espacio suficiente en el disco duro para poder ejecutar sus aplicaciones.

e) La instalación de software y/o sistemas sólo podrán ser efectuadas por la Oficina de Planeación y Sistemas, siendo ésta quien efectúe las pruebas técnicas de la instalación, así como su mantenimiento y respaldos.

f) Se debe respetar la propiedad intelectual y licencias. El usuario no podrá copiar o redistribuir programas propiedad de la Cámara de Representantes.

g) La instalación de un software y/o Sistema no autorizado por la Oficina de Planeación y Sistemas, puede provocar que alguna aplicación no funcione adecuadamente, siendo responsabilidad absoluta del usuario del equipo.

## 9. POLÍTICAS DE SEGURIDAD DE SERVICIO AL USUARIO:

a) Es responsabilidad de los usuarios cuidar y mantener el buen estado de los equipos computacionales.

b) La Oficina de Planeación y Sistemas, respaldará periódicamente la información que se encuentra en los distintos servidores.

c) Los usuarios deberán utilizar únicamente los servicios para los cuales está autorizado. No debe utilizar la cuenta de otro usuario, ni intentar apoderarse de claves de acceso de otros, como tampoco intentar burlar los sistemas de seguridad bajo ningún punto de vista.

d) El usuario deberá tramitar el usuario de Dominio y cuenta de correo institucional con la Oficina de Planeación y Sistemas por escrito con la previa autorización del Jefe inmediato.

e) Cada usuario de un PC o LAPTOP será responsable de mantener los debidos resguardos en cuanto a confidencialidad de los datos almacenados.

f) No utilizar el nombre de otro usuario ocultando el propio bajo ninguna circunstancia al momento de utilizar los servicios informáticos institucionales.

g) El usuario deberá respetar a los demás usuarios. Los archivos, discos, información y datos en otras formas individuales, son privados; no se debe leer, copiar, o cambiar los archivos de cualquier usuario, a menos que haya sido autorizado por éste.

## 10. POLÍTICAS DE USO DE INTERNET

El objetivo de esta política es otorgar un ordenamiento en el uso del servicio de internet, definiendo de manera general, no limitativa, las actuaciones consideradas como abusivas y prohibidas.

a) Las configuraciones de las estaciones de trabajo para acceder al servicio de Internet son responsabilidad exclusiva del personal de la Oficina de Planeación y Sistemas.

b) La Oficina de Planeación y Sistemas tiene el deber de filtrar todo contenido que vaya en contra del interés de la Cámara de Representantes.

c) La Oficina de Planeación y Sistemas tiene la autoridad para controlar y negar el acceso a cualquiera que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

d) El uso de Internet es personal e intransferible no permitiéndose que terceras personas hagan uso del servicio.

e) Cada usuario es el responsable de las acciones efectuadas a través de este servicio.

f) La Información consultada en cualquier horario de trabajo a través de Internet, debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del usuario y/o servir como herramienta para desempeñar sus funciones.

g) El usuario no debe utilizar ninguna conexión privada a Internet a través de las estaciones de trabajo conectadas simultáneamente a redes de la Cámara de Representantes (conexiones celulares).

h) Se prohíbe utilizar los servicios de red para juegos (en línea) a través del servicio de Internet o Intranet.

i) Se prohíbe acceder a redes sociales en las horas laborales.

j) Se prohíbe acceder a lugares obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros.

k) Los mensajes que se envíen vía Internet, serán 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 ésta u otra Institución.

l) Está prohibido bajar (download), instalar, copiar o almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor.

m) Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que tal información esté cifrada.

n) De manera consistente con prácticas generalmente aceptadas, el Data Center procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la red en el uso de Internet contienen detalles sobre lugares de acceso, número de veces, duración, y fecha y hora en que se efectuó el acceso.

o) Es política de la Oficina de Planeación y Sistemas no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria.

p) La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la entidad.

q) Está prohibido ver o bajar archivos de música o vídeo desde Internet.

## 11. POLÍTICAS DE USO DE CORREO ELECTRÓNICO

El servicio de correo electrónico es una plataforma de comunicación brindada por la Dirección Administrativa y la Oficina de Planeación y Sistemas, la cual permite a los usuarios enviar y recibir mensajes a todo el mundo electrónicamente. Este servicio se utiliza para mejorar la comunicación entre los funcionarios/empleados y entre entidades públicas o privadas.

El objetivo de esta política es otorgar un ordenamiento en el uso del servicio de correo electrónico, definiendo de manera general, no limitativa, las actuaciones consideradas como abusivas y prohibidas.

a) Es responsabilidad del usuario mantener la confidencialidad de la clave de acceso.
b) La Oficina de Planeación y Sistemas en caso de uso no permitido del correo electrónico, suministrará la información del usuario a la entidad que lo requiera para algún tipo de investigación por uso no apropiado del servicio.
c) La cuenta de correo es personal e intransferible no permitiéndose que otros empleados hagan uso de ella.
d) Cada usuario es el responsable de las acciones efectuadas en su cuenta de correo; la Oficina de Planeación y Sistemas no se hace responsable por las opiniones emitidas.
e) Es responsabilidad del usuario realizar administración de su cuenta periódicamente para que exista espacio disponible.
f) Todo usuario es responsable por los datos/documentos adjuntos que envía.
g) El incumplimiento por parte del usuario puede ocasionar la suspensión y posterior baja del sistema del servicio de correo electrónico.
h) Es estrictamente prohibido el envío de cadenas.

### 11.1 Reenvío de mensajes:

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Institución, se debe ejercer cierta cautela al reenviar los mensajes. En todo caso no debe remitirse información confidencial de la Cámara de Representantes sin la debida aprobación.

### 11.2 Borrado de mensajes:

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. Y es responsabilidad de cada usuario salvaguardar la información propia de sus labores.

## 12. POLÍTICAS DE SEGURIDAD PARA REDES

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la institución al estar conectada a redes de computadoras. Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Cámara de Representantes.

a) Todos los cambios en los servidores y equipos de red de la Cámara de Representantes, incluyendo la instalación de un nuevo software y otros, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

b) Los privilegios especiales, de 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.

c) Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. La Oficina de planeación y Sistemas debe revocar rápidamente los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

d) Cuando un funcionario o contratista se retira o termina su contrato con la Cámara de Representantes, debe diligenciar el FORMATO "Paz y Salvo por Prestación de Servicios Personales y Funcionarios A-G-1-F4" que puede ser descargado de la página WEB o Intranet y tramitarlo ante la Oficina de Planeación y Sistemas para que se desactive la cuenta de usuario.

## 13. POLÍTICAS DE SEGURIDAD PARA CONTRASEÑAS Y EL CONTROL DE ACCESO

a) El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y 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.

b) No 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.

c) 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.

d) 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.

e) 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.

f) Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

g) Las contraseñas deben cambiarse con frecuencia, siendo éstas de uso personal, será de responsabilidad de cada usuario acordarse de la contraseña.

h) Toda contraseña debe empezar con una letra, seguida de un conjunto de caracteres (letra, número o símbolo). Sé recomienda no usar contraseñas que sean fácilmente deducibles.

i) Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto, la sesión debe ser inmediatamente desconectada.

j) Para el acceso remoto a los recursos informáticos de la entidad la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas.

k) Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 05 minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña.

l) Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

m) Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Cámara de Representantes pudiendo ser causal de despido.

n) Para tener evidencias en casos de 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.

o) Los archivos de bitácora (logs) y los registros de auditoria (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.

p) Los servidores de red deben estar ubicados en sitios apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos sitios y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas lectoras de proximidad).

## 14. TIPOS DE FALTAS

En situaciones de incumplimiento y/o violación a las políticas de seguridad de la Información se deberá tramitar el cumplimiento de la ley 734 de 2002, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

Las faltas cometidas por los usuarios serán sancionadas de acuerdo a la gravedad de las mismas y se clasifican en leves, menos graves y graves; según se señalan a continuación:

### a) LEVES

a) Usar los equipos de la Institución, para actividades no laborales como juegos y pasatiempos.

b) Manipular alimentos sobre los equipos de cómputo.

c) Utilizar fondos y/o protectores de pantalla que no son los institucionales (personalizados), sean computadores personales y/o portátiles, propiedad de la Cámara de Representantes.

d) Exponer los equipos a riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

e) No reportar inmediatamente fallas en los computadores o en la red que consecuentemente causen problemas serios como pérdida de la información o indisponibilidad de los servicios.

f) Mover (cambiar de lugar, desplazar) los equipos o reubicarlos sin autorización previa.

g) No reportar a la Dirección Administrativa o a la Oficina de Planeación y Sistemas la detección de, virus u otro agente potencialmente peligroso.

h) La no utilización de un programa antivirus para examinar todo archivo que venga de afuera o inclusive de otras Direcciones o dependencias de la Cámara de Representantes.

i) Utilizar Memorias USB u otros medios de almacenamiento en cualquier computador portadores de virus u otros agentes dañinos sin escanear previamente.

j) Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.

k) La falta de cuidado, pulcritud y limpieza del equipo de informática asignado.

l) La navegación en Internet para fines personales por períodos prolongados de tiempo.

m) Bajar archivos de música o vídeo desde Internet.

## b) MENOS GRAVES:

Constituyen faltas menos graves:

a) La reincidencia en la comisión de una falta leve

b) Modificar la configuración de hardware y/o software establecida por la Dirección Administrativa o la Oficina de Planeación y Sistemas.

c) La instalación de programas y la modificación de los programas, paquetes y configuraciones ya instalados en los computadores.

d) Visitar o acceder a sitios web obscenos, que distribuyan material pornográfico, o materiales ofensivos en perjuicio de terceros.

e) Utilizar el Internet para enviar mensajes que vayan en contra de empleados y/o de los intereses de otras personas, así como de ésta u otra Institución. Por ejemplo (cadenas correos masivos).

## c) GRAVES:

Constituyen faltas graves:

a) La reincidencia en la comisión de una falta menos grave

b) La pérdida o robo de cualquier componente de hardware o programa de software por negligencia o dolo debidamente comprobado.

c) Revelar datos confidenciales.

d) Hacer copias o usar software tanto adquirido como desarrollado, para fines personales y en violación a derechos de autor.

e) Hacer uso de software bajado de Internet (software libre, gratis, demos, etc.) y en general software que provenga de una fuente no confiable.

f) El uso de módems en PCs que tengan también conexión a la red local (LAN.

g) Copiar a un medio removible (como un DVD, USB, CD), el software o los datos residentes en las computadoras de la Cámara de Representantes, sin la aprobación previa.

h) No realizar respaldos de los datos guardados en PCs y servidores.

i) Negligencia en el manejo de la información confidencial de la Cámara de Representantes contenida en computador personal o portátil.

j) Borrar/eliminar la información original no cifrada sin que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

k) Utilizar/usurpar el acceso a las claves utilizadas para el cifrado y descifrado.

l) Abrir los equipos de cómputo, violentar sellos.

m) Prestar, compartir, usurpar la contraseña.

n) Burlar los sistemas de seguridad informática.

o) Sacar (extraer) o cambiar componentes de los equipos

p) Prestar e intercambiar los equipos de cómputo sin la correspondiente autorización.

q) Instalar equipos sin la supervisión y autorización expresa de la Oficina de Planeación y Sistemas.

r) Leer, copiar, o cambiar los archivos de cualquier otro usuario.

s) Inspeccionar, copiar y almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor.

t) Enviar a través de Internet mensajes con información confidencial a menos que tal información esté cifrada y autorizada.

u) Divulgar, duplicar, modificar, destruir, extraviar, robar y acceder a información confidencial.

## 15. RESPONSABLE DEL DOCUMENTO

Jefe de Planeación y Sistemas Cámara de Representantes