CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

RESOLUCIÓN Nº 2345 de 2010

20 SET. 2010

"Por medio de la cual se determinan y adoptan las Políticas de Seguridad aplicada a la Honorable Cámara de Representantes, en el uso de los equipos de cómputo, los servicios institucionales de Correo Electrónico e Internet, el manejo, instalación y desinstalación de software y la conservación y cuidado de la información institucional"

CONSIDERANDO

Que con el fin de proteger los activos de la corporación en materia informática, se hace indispensable establecer unas políticas de seguridad, mediante las cuales se determinan las condiciones y conductas mínimas de uso de los activos informáticos por parte de los funcionarios adscritos a la Cámara de Representantes.

Que por ser los activos informáticos y entre estos el Hardware y el Software, las herramientas principales para el desarrollo de las actividades de la Cámara de Representantes, por lo tanto el uso inadecuado de los recursos tecnológicos expone a la Entidad a riesgos de pérdida y/o daño de equipos e información, propagación de virus; comprometiendo los servicios, las redes y la imagen de la Institución y considerando la vulnerabilidad de la información mediante su utilización, es preciso desarrollar un conjunto de normas de actuación que conformen las políticas de seguridad informática, lo cual garantiza la integridad de dichos bienes que redunda en un mejor desempeño laboral, permitiendo a su vez cumplir con la misión de la corporación.

Con el fin de ilustrar de manera óptima a los funcionarios y colaboradores de la Cámara de Representantes, es necesario establecer unas políticas de seguridad que regulen el uso adecuado de los recursos y activos informáticos de la Cámara de Representantes.

RESUELVE:

ARTICULO PRIMERO: Aprobar y adoptar para la Cámara de Representantes, las Políticas de Seguridad de la red de sistemas Corporativa.

La seguridad de la información se define como la preservación de los siguientes componentes: la confidencialidad, en donde se garantiza que la información sea accesible sólo a las personas autorizadas; integridad, se logra estableciendo métodos (por ejemplo: back up´s) para proteger la información; y la disponibilidad, para garantizar a los usuarios autorizados tengan acceso a los servicios informáticos prestados por la H. Cámara de Representantes.

La seguridad informática ha tomado un gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las entidades para mejorar su productividad y poder explorar mas allá de las fronteras, lo cual lógicamente ha traído consigo, la aparición de nuevas de amenazas para los sistemas de información.

Estos riesgos que se enfrentan, han llevado a que muchas entidades desarrollen documentos, directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la Cámara de Representantes.

La globalización ha exigido el desarrollo de las telecomunicaciones permitiendo un mayor y mejor flujo de información, que a su vez hace necesaria la instauración de políticas y métodos que la protejan ante los riesgos de saboteo, robo o eliminación.

"El reglamento de seguridad basado en la Norma ISO IEC 27001, engloba los objetivos, conductas, normas, métodos de actuación y distribución de responsabilidades ya que es necesario que el funcionario de la Honorable Cámara de Representantes posea sentido de pertenencia y con el ánimo de promover el cumplimiento de las actividades proveer, administrar y soportar los servicios informáticos necesarios para apoyar la operación y la toma de decisiones de la entidad cumpliendo con la Misión de la Honorable Cámara de Representantes y contribuyendo a su progreso. Razón por la cual la Oficina de Planeación y sistemas, da a conocer las siguientes políticas de seguridad a tener en cuenta en el área de trabajo, con el fin de lograr un mejor desempeño de la Cámara de Representantes.

ARTICULO SEGUNDO: DEL USO ADECUADO. Los usuarios de la infraestructura informática propiedad de la H. Cámara de Representantes deberán acogerse a las normas de uso que a continuación se exponen, en busca de salvaguardar la integridad de los equipos y la información que en ellos se aloja.

- Los usuarios de la red deberán adoptar las políticas de seguridad establecidas y difundidas por la Oficina de Planeación y Sistemas de la H. Cámara de Representantes.

- No dar información confidencial de la H. Cámara de Representantes ni permitir y/o facilitar el uso de los sistemas informáticos a personas no autorizadas.

- No utilizar los recursos informáticos y de telecomunicaciones para actividades ajenas que no estén directamente relacionadas con el trabajo.

- Reportar inmediatamente a su jefe inmediato y a la Oficina de Planeación y Sistemas cualquier evento que pueda comprometer la seguridad de la red de la H. Cámara de Representantes y sus recursos informáticos.

- No está permitido el uso de módems en equipos de escritorio (PCs, Terminales, estaciones de trabajo etc...) que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado por la Oficina de Planeación y Sistemas.

- Se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite la descarga ni el uso de software de distribución gratuita, tampoco se permite el uso del software no licenciado, a menos que haya sido previamente aprobado por la Oficina de Planeación y Sistemas.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Almacén y a la Oficina de Planeación y Sistemas.

- Está terminantemente prohibido hacer copias o usar el software de la H. Cámara de Representantes para fines personales, porque está protegido por derechos de autor y requiere licencia de uso.

- Las solicitudes de creación, modificación y eliminación de usuarios para los Sistemas de Información, se realizan mediante oficio autorizado por el jefe de la dependencia y dirigido al Jefe de la Oficina de Planeación y Sistemas.

ARTICULO TERCERO: CORREO ELECTRÓNICO INSTITUCIONAL. Los lineamientos que a continuación se dictan, están enfocados hacia el uso seguro del correo institucional y del tráfico de la información adjunta.

- La creación de las cuentas de usuario tendrán la siguiente forma: primernombre.primerapellido@camara.gov.co

  Por ejemplo: Para el funcionario Jesús Emilsen Pinzón Ortiz, su cuenta de correo se crearía de la siguiente manera jesus.pinzon@camara.gov.co.

  Como contraseña inicial tendrá el número de la cedula de ciudadanía o documento de identidad. Se debe hacer la aclaración de que una vez sea recibida la notificación de la creación de la cuenta ya sea vía telefónica o escrita mediante un OPS, el usuario debe hacer cambio de la contraseña.

  Las solicitudes de creación y/o eliminación de cuentas debe ser dirigido al Jefe de Planeación y Sistemas de la corporación y autorizadas exclusivamente por él.

- No se deben ejecutar archivos que vengan adjuntos en mensaje de emisor desconocido, sospechoso o poco confiable.

- No debe remitirse información confidencial fuera de la Honorable Cámara de Representantes sin la pertinente autorización del responsable de la dependencia.

- No se debe usar el correo electrónico para enviar o recibir mensajes tipo spam o hoax.

- Administrar adecuadamente la bandeja del buzón del correo electrónico institucional con el fin de no saturarla, mediante una revisión periódica y eliminación de los mensajes poco relevantes ya leídos. Las bandejas del buzón del Correo Electrónico Institucional deben ser revisadas periódicamente y los mensajes contenidos en ellas borrados una vez sean leídos. Si hay necesidad de conservarlos, los mensajes se deberán grabar en un sitio destinado para su almacenamiento; esto también se aplica a los correos enviados y a la papelera de

reciclaje. Así mismo, cuando las unidades requieran compartir un archivo, se sugiere hacerlo utilizando las herramientas pertinentes, en vez de enviarlo por correo.

- Se debe verificar la presencia de software malicioso en archivos adjuntos a mensajes de correo electrónico antes de su uso. Adicionalmente, todo mensaje sospechoso respecto de su remitente o contenido debe ser ignorado y eliminado sin abrirlo, ya que puede ser contentivo de virus, en especial si contiene archivos adjuntos (attach) con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias eróticas o alusiones a personajes famosos.

- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la mesa de ayuda a la extensión 4444 y 5050, o al correo electrónico soporte.tecnico@camara.gov.co.

- El usuario que NO haga uso de su cuenta de correo por un periodo superior a 90 días, el sistema automáticamente la deshabilitará. La reactivación de dicha cuenta deberá solicitarse mediante oficio al Jefe de Planeación y Sistemas, y si éste autoriza se remitirá dicha solicitud al administrador de la red del centro de cómputo.

Parágrafo1: Al crear las cuentas de Correo Electrónico Institucional, la Oficina de Sistemas establecerá criterios de restricción, de acuerdo con las funciones o perfil del usuario, a efectos de racionalizar la capacidad del buzón, delimitar la posibilidad de enviar mensajes colectivos o a distintos grupos, orígenes o destinatarios, entre otras medidas.

Parágrafo 2: La H. Honorable Cámara de Representantes no asume responsabilidad alguna por los contenidos emitidos a través del correo electrónico o por el uso ilegal y mal intencionado por parte de los usuarios.

Se sugiere aclarar que la corporación no se hace responsable del uso indebido que el usuario haga de su contraseña privada. La responsabilidad de la corporación va hasta el momento en el que se hace entrega de la primera contraseña al usuario mediante oficio formal.

Las contraseñas deben cumplir con unos estándares de seguridad que disminuyan su vulnerabilidad.(mínimo 6 caracteres alfanuméricos, con palabras que no pertenezcan al diccionario, adoptando el uso de mayúsculas y minúsculas combinadas)

ARTICULO CUARTO: INTERNET. El servicio de Internet suministrado por la H. Cámara de Representantes es una herramienta de apoyo para el desarrollo de las funciones institucionales, sin embargo, su uso está sometido al cumplimiento de la normas que a continuación se enuncian:

- La administración del servidor de Internet y/o servidor WEB, servidor INTRANET y servidor de Correo electrónico, así como de los permisos y autorizaciones de páginas, es responsabilidad de la Oficina de Planeación y Sistemas.

- Las diferentes dependencias que tengan contenidos en la Web tendrán un único responsable de manejo de página Web, con su respectivo usuario y clave con el fin de restringir el acceso.

- Se hará periódicamente una revisión del contenido de la página Web, con el fin de eliminar artículos obsoletos y mantener los boletines y noticias actualizadas.

- Está prohibido el uso del Internet para hacer proselitismo, mercadeo, o cualquier otra actividad que atente contra y las buenas costumbres.

- A los administradores de los servidores de Web corresponde la verificación de respaldo y protección adecuada.

- El uso del Internet debe estar encaminado al desarrollo de las actividades únicamente laborales, y no para el entretenimiento personal.

- Se garantizar el correcto funcionamiento de la página Web corporativa en los navegadores Web de Microsoft Explorer 8 y Mozila 3.5.

ARTICULO QUINTO: LA RED DE SISTEMAS. La Red de la H. Cámara de Representantes, centraliza los servicios requeridos por los diferentes usuarios y se compone del cableado estructurado y de los servidores con sus respectivos aplicativos, útiles para la gestión legislativa y administrativa de la entidad. Su manipulación está reglamentada por:

- La persona que utilice los servicios que ofrece la red WAN y/o VPN deberá conocer y aceptar el reglamento vigente sobre su uso.

- Los usuarios de los recursos de la red (Cables, enlaces, equipos activos y/o pasivos) y el acceso a los centros de cableado de los edificios, no podrán realizar intervención física sobre estos.

- Se requiere usar protectores contra transitorios de energía eléctrica y en los servidores usarse fuentes de poder ininterrumpible (UPS).

- Los tomas naranja (reguladas) deben ser utilizadas exclusivamente para conectar la CPU (torre) y el monitor de cada computador. Elementos como fotocopiadoras, multifuncionales, televisores, neveras, celulares, reguladores de voltaje, PC Portátiles, etc, deben conectarse a las tomas blancas (no reguladas).

- La Oficina de Planeación y Sistemas realizará las restricciones de acceso a ciertos servicios, en procura de mejorar el rendimiento de la red. Se sugiere especificar claramente sobre que servicios, páginas, sitios Web, aplicativos y demás se realizaran las restricciones, para así evitar futuros inconvenientes con los usuarios.

- Respetar la privacidad de otros usuarios. No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin su consentimiento.

- Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la

seguridad informática de la Cámara de Representantes, a través de medio físico o electrónico alguno.

- Se prohíbe salvo con autorización y supervisión expresa de la Oficina de Planeación y Sistemas, la intervención física de los usuarios sobre los recursos de la red (Cables, enlaces, equipos activos y/o pasivos) y el acceso a los centros de cableado del edificio.

- Tampoco está permitida la instalación de cables, derivaciones a través de conectores en "T", enrutadores, hubs o cualquier tipo de derivación de voz o datos por parte de los usuarios. Así mismo, no se permite la instalación de ningún servicio que intervenga directamente el cableado que alimenta las tomas.

- La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser adelantada por personal autorizado por la Oficina de Planeación y Sistemas.

- Los recursos disponibles a través de la Red de la Honorable Cámara de Representantes serán de uso exclusivo para asuntos relacionados con las actividades que allí se generen

- Es necesario tener actualizada la documentación como los mapas topológicos de red donde enmarque los puntos de red y su interconexión, puntos de enlaces, velocidades, dispositivos, nivel de ancho de banda ocupado.

- Todos los cambios en los servidores y demás equipos de red de la H. Cámara de Representantes, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, deben ser documentados y debidamente aprobados por la Jefatura de Planeación y Sistemas.

- Los equipos del centro de cómputo necesitan contar con condiciones ambientales adecuadas, contar con protección contra incendios detectores de humo, extintores, control de clima (de 18 a 20 grados centígrados, aconsejable 20 grados), control de humedad (el rango 20% a 50% de humedad).

SEGURIDAD DEL CABLEADO

Se debe proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información de interceptaciones o daños.

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben tener en lo posible una adecuada protección alternativa.

- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.

- Se deben separar los cables de energía de los de telecomunicaciones esto para evitar posibles interferencias o generación de ruido.

- Es necesario rotular adecuadamente los cables para que sean claramente identificables, además de minimizar errores de manejo.

- Es necesario tener una documentación del rotulado del cableado estructurado de la Cámara de Representantes, con el fin de minimizar la posibilidad de errores en su manejo.

PARAGRAFO: El tendido del cableado esta en manos de un socio colaborador de la Corporación; el cual deberá transferir la propiedad de los dispositivos activos y pasivos de la red, con manuales una vez se cumpla la parte contractual y el conocimiento en el manejo y administración de la misma por lo menos tres meses antes de finalizar la parte contractual (el convenio).

SUMINISTRO ELÉCTRICO

- No debe conectar el equipo a la corriente no regulada, debido a que esto puede ocasionar daños irreparables. Si por algún motivo, no hay disponibilidad de tomas reguladas (Tomas Color Naranja), se recomienda conectar el equipo de computo a la toma No regulada (toma naranja) mediante un estabilizador de voltaje. De la misma manera los electrodomésticos no deben ser conectados a la corriente regulada porque ocasiona daños a los equipos electrónicos.

- No se debe recargar una toma eléctrica (Multitomas, Extensiones Eléctricas, etc) con múltiples equipos eléctricos y/o electrónicos.

- Los servidores activos de la unidad y los Backus deben estar en todo momento conectados a la toma regulada.

- En el evento de suspenderse el fluido eléctrico, los equipos que no se encuentran amparados por la U.P.S. (Planta para equipos de cómputo), quedarán sin funcionamiento. Por lo tanto, es necesario apagar completamente las pantallas, computadores e impresoras hasta cuando el encargado del área autorice nuevamente su encendido.

- No se debe encender el equipo inmediatamente se establezca la energía, ya que ésta puede llegar con alto voltaje, lo cual podría quemarlos. Se recomienda esperar un tiempo prudencial (5 minutos) para encenderlos.

SEGURIDAD EN CONEXIONES TERMINALES

INTRANET

- El acceso lógico a la Intranet debe ser administrado por la Oficina de Planeación y Sistemas.

- Validar usuarios y contraseñas.

- Especificar perfiles según el usuario, y así mostrar los diferentes accesos a la información.

- Las sesiones deben desactivarse tras un periodo definido de inactividad.

- Se garantizara el buen funcionamiento de la intranet en el navegador Explorer 8 de Microsoft, y se tomara como software oficial para este servicio.

VPN's

- El acceso lógico a la VPN debe ser administrado por la Oficina de Planeación y Sistemas.
- Se debe utilizar un sistema de autenticación de factores múltiples de acceso remoto que limite el acceso únicamente a aquellos usuarios que deban conectarse por motivos laborales. Se sugiere que por seguridad no se permita el acceso externo a la "INTRANET".
- Se deben crear grupos para asignación de privilegios o permisos a los aplicativos críticos
- Toda persona que utilice los servicios que ofrece la VPN deberá conocer y aceptar el reglamento vigente sobre su uso.

ARTICULO SEXTO: LOS EQUIPOS DE SISTEMAS. Todos los componentes del hardware de la H. Cámara de Representantes están para el servicio de los funcionarios, pero también recae sobre ellos la responsabilidad de su uso adecuado. Para ello se conformo el siguiente conjunto de reglas:

- La Oficina de Planeación y Sistemas deberá dar cumplimiento a los procedimientos de ingreso, instalación, reasignación, reubicación y todo aquello que implique movimiento físico de los equipos. No debe hacerse movimiento de los equipos o reubicación de los mismos sin previa autorización de la Sección de Suministros con el fin de llevar el control individual de inventarios y la Oficina de Planeación y sistemas, para el manejo de las hojas de vida de los equipos. Para llevar un equipo fuera de las instalaciones o dentro de las diferentes dependencias se requiere una autorización escrita de la sección de suministros y la Oficina de Planeación Sistemas. De otro lado, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de cada dependencia, (la oficina de Planeación y Sistemas es la encargada de reasignaciones, y la Sección de Suministros la encargada del inventario).
- Es responsabilidad del funcionario a quien se le ha asignado el equipo, su protección e integridad, y en caso de fallas en el desempeño del mismo, debe comunicarlo a la mesa de ayuda de la Oficina de Planeación y Sistemas.
- Los computadores portátiles, laptops y cualquier equipo que se pueda conectar a la red de la institución deben ser estar protegidos con sistemas antivirus actualizados para minimizar el riesgo de propagación de virus y software mal intencionado o ser escaneados con un programa antivirus antes de conectarse a la misma. No debería permitirse la libre conexión a la red de equipos de computo ajenos a la corporación, salvo los que autorice la Jefatura de Planeación y Sistemas, debido a que el Ancho de Banda Actual y la infraestructura de red está diseñada para la conexión de un determinado número de equipos. De no ser posible esta restricción se debe realizar un aumento progresivo del canal del Ancho de Banda de Internet.

- Solo personas autorizadas pueden ingresar al centro de cómputo para seguridad de la información, de los servidores y sus demás componentes. Y debe registrar en la bitácora del centro de cómputo, las actividades realizadas en los servidores.
- Se deberá tener presente los documentos de garantía y de pólizas de los equipos de red.
- La Oficina de Planeación y Sistemas debe establecer cronogramas periódicos de mantenimiento preventivo a razón de dos veces por año (semestral).
- Efectuar la relación de equipos de cómputo de la H. Cámara de Representantes cada seis meses.
- Cualquier falla, pérdida o robo de equipos u otros elementos de la red, deben reportarse inmediatamente a la Oficina de Planeación y sistemas a la extensión 5152, o al correo electrónico sistemas@camara.gov.co, en el horario: de lunes a viernes de 8:00am a 6:00pm.

SEGURIDAD DE LOS EQUIPOS

- Los equipos deben situarse donde se minimicen los accesos innecesarios a las áreas de trabajo.
- Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.
- Mantener en un lugar visible y a conocimiento del personal de la Oficina de Planeación y sistemas, el equipo para la extinción de incendios.
- Mantener presente los documentos de garantía y de pólizas de los equipos de red.
- Capacitar al personal en el empleo de extintores, sistemas de alarma y cualquier mecanismo de seguridad.
- Mantener el servidor de backup en el centro de cómputo, mantener en un lugar seguro las carpetas de software y licencias de las máquinas.

MANTENIMIENTO DE EQUIPOS

Los equipos deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

- El equipamiento debe mantenerse de acuerdo con los intervalos servicio y especificaciones recomendados por el proveedor.
- Solo el personal de mantenimiento debidamente autorizado debe realizar la reparación y servicio de los equipos.

- Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.

ARTICULO SÉPTIMO: SEGURIDAD DE HARDWARE Y SOFTWARE. El uso de los equipos y aplicativos licenciados por la H. Cámara de Representantes, acarrea con responsabilidades de orden penal, administrativo y disciplinarias, por cuanto, los funcionarios están en la obligación de acoger la siguiente normatividad:

- El código de ingreso es de carácter personal e intransferible; por lo tanto, no debe ser revelado a otros funcionarios.

- Es responsabilidad de cada funcionario toda modificación de información realizada desde su cuenta de usuario, debido a que su clave es de uso exclusivo e intransferible, Y por seguridad debe cambiarse periódicamente por el usuario.

- Los equipos deben estar apagados durante los tiempos prolongados de no uso. Se recomienda realizar apagado del PC y Monitor al termino de la jornada laboral.

- Cualquier inconveniente con los componentes de los equipos debe ser reportado a la mesa de ayuda de la Oficina de Planeación y Sistemas. Se recomienda al usuario que realice backups periódicos de su información para evitar pérdidas ocasionadas por algún tipo de falla en el equipo. La responsabilidad de la información almacenada en el PC y el Backup de la misma es única y exclusivamente de cada funcionario.

- La totalidad de los equipos deben ser conectados a las fuentes de poder regulada (los reguladores externos no deben ser conectados a las tomas naranjas "reguladas") destinadas para ello y a su vez están conectadas a la UPS de cada edificio. De la misma manera los electrodomésticos no deben ser conectados a la corriente regulada porque ocasiona daños a los equipos electrónicos. No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multitomas a las mismas.

- La intervención de los equipos es exclusiva del personal de soporte técnico de la mesa de ayuda de la Oficina de Planeación y Sistemas, por tanto no se permiten modificaciones o intercambio de componentes realizados por los funcionarios. Los únicos autorizados para realizar modificaciones a la configuración original de los equipos, así como para destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, conocer las contraseñas de administrador, son los funcionarios de la Oficina de Planeación y Sistemas y/o las personas por ellos autorizadas. no es permitido intercambiar elementos como teclados, parlantes, monitores, etc. Sin previa autorización del encargado del área informática.

- La instalación o desinstalación de programas es responsabilidad exclusiva del personal autorizado de la Oficina de Planeación y Sistemas.

- Solamente la información de carácter institucional, relacionada con la realización de las labores para cada empleo, puede ser almacenada en los equipos que pertenecen a la H. Cámara de Representantes.

- Verificar que los nuevos equipos que se adquieran sean compatibles con las plataformas de Hardware y Software de la red de sistemas de la H. Cámara de Representantes.

- Es obligación de los funcionarios o contratistas retornar los activos de la Cámara de Representantes que estén en su posesión, al momento de finalizar su vinculación con la H. Cámara de Representantes.

- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los equipos de sistemas asignados.

- Durante la jornada laboral y en todo tiempo de uso, corresponde al funcionario prestar la debida custodia y cuidado a los equipos de cómputo asignados, así como impedir su sustracción, destrucción, ocultamiento o utilización indebida.
- Cualquier pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada de inmediato a la Dirección Administrativa, División de Servicios, la Oficina de Planeación y Sistemas y la Sección de Suministros, para los fines pertinentes, por el funcionario que tenga a cargo el equipo.

ARTICULO OCTAVO: EL SOFTWARE. La información es el activo más importante de las organizaciones, por cuanto se debe asegurar su protección contra robo, modificación malintencionada y pérdidas accidentales. Para ello, es de obligatorio cumplimento el siguiente conjunto de normas:

- La Oficina de Planeación y Sistemas es la responsable de revisar y ejecutar diariamente la existencia de actualizaciones del antivirus.

- Es obligación de la Oficina de Planeación y Sistemas realizar dos veces a la semana las copias de seguridad de la información contenida en los aplicativos Kactus (Aplicativo de nómina) y Seven (aplicativo de inventarios y activos fijos), tal como se contempla en el procedimiento "PLAN. 02.03.01 Back Up archivos Kactus y Seven de la H. Cámara de Representantes".

- Las copias de seguridad de los aplicativos y sus bases de datos deben ser almacenadas con suficientes medidas de seguridad y llevar inventario de todos los dispositivos de almacenamiento secundario con la identificación de su contenido y versión.

- Los usuarios de los equipos de cómputo de la H. Cámara de Representantes, son responsables del manejo de su información y de la protección de los programas y datos contra pérdida o daño.

- Las aplicaciones deben ser actualizadas según las versiones liberadas por el proveedor o desarrollador, con el fin de corregir las fallas, mejorar el rendimiento de los aplicativos y atender cambios del Gobierno central. Esto es realizado únicamente por personal autorizado por la Oficina de Planeación y Sistemas.

- Para las actualizaciones del software antivirus, se sugiere realizar esta acción todos los días en el lapso de tiempo de las 12:30 m a 2:00 p.m.; ya que se cuenta con computadores obsoletos y en otras horas de trabajo puede ocasionar lentitud en el proceso de los equipos.

- Se prohíbe la realización de copias del software institucional para fines personales. La Oficina de Planeación y Sistemas es la única dependencia

autorizada para realizar copia de seguridad del software licenciado por la Entidad.

- En ausencia prolongada del funcionario usuario del equipo y en la hora de almuerzo, debe bloquearse el computador; de lo contrario se expone la información a acceso de terceros, daño, alteración o uso indebido, así como a la suplantación del usuario original. Para el caso del protector de pantalla se debe configurar su activación al cabo de 15 minutos de inactividad requiriendo de una contraseña para reanudar la actividad. Además es conveniente cerrar su sesión manualmente cada vez que se ausente de su estación de trabajo por un tiempo considerable.

- Debe respetarse y no modificarse la configuración de software instalado y asignado por la Oficina de Planeación y Sistemas. En caso de ser requerido, solamente puede ser realizado por funcionarios autorizados por esta misma Oficina.

- Todo el software de la Honorable Cámara de Representantes está protegido por derechos de autor y requiere licencia de uso. De la misma manera queda terminantemente prohibido hacer copias de software para fines personales. La Oficina de Sistemas es la única dependencia autorizada para realizar copia de seguridad del software licenciado por la Entidad.

- Está prohibido instalar, ejecutar y/o utilizar programas o herramientas de software o hardware que:

- Adivinen las contraseñas alojadas en las tablas de usuarios de equipos locales o remotos.

- Monitoreen la actividad de los sistemas informáticos de equipos locales o remotos. Se excluye de esta prohibición las herramientas de software y hardware que utilice la Oficina de Planeación y Sistemas con el único propósito de administrar la funcionalidad y la seguridad de los recursos informáticos de la Cámara de Representantes.

- Rastreen vulnerabilidades en sistemas de cómputo (hardware o software). Se excluye de esta prohibición las herramientas que utilice la Oficina de Planeación y Sistemas con el único propósito de evaluar la seguridad de los recursos informáticos de la corporación.

- Exploten alguna vulnerabilidad de un sistema informático para acceder así a privilegios que no han sido explícitamente otorgados por el administrador de la red o de un recurso informático en particular.

- Todo funcionario es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.

- El software y hardware instalado en los equipos de cómputo de la Honorable Cámara de Representantes no debe ser utilizado con propósitos ilegales, no autorizados, personales o ajenos a la misión de la corporación.

INFORMACIÓN RELEVANTE

- No debe extraerse información de las aplicaciones relevantes (SIIF y demás bases de datos) de las instalaciones sin la aprobación previa del jefe de cada dependencia. Aplica para todos aquellos que se encuentren conectados a la red de la Cámara de Representantes, Internet o que posean equipos portátiles.

- Mantendrán en reserva la documentación e información que por razón de su empleo, cargo o función, conserven bajo su cuidado o a la cual tengan acceso; evitarán su sustracción, destrucción, ocultamiento o utilización indebida; se abstendrán de alterarla, falsificarla, ocultarla o borrarla, e impedirán que terceros no autorizados ejecuten tales acciones sobre la misma.

- No debe utilizarse software descargado de sitios desconocidos de Internet, ni debe instalarse software no autorizado por el área informática. Recuerde que cualquier software no oficial es responsabilidad directa del poseedor y acarrea consecuencias penales y pecuniarias.

- Periódicamente debe hacerse el respaldo de la información correspondiente al trabajo de la Honorable Cámara de Representantes y dichas copias deben guardarse en un lugar seguro.

- Los archivos que ya no se necesiten deben ser eliminados periódicamente de su área de almacenamiento. Con esto se libera espacio en disco y se reducen los riesgos de acceso no deseado a dicha información.

- El funcionario que utilice un computador portátil que contenga información confidencial de la Cámara de Representantes, deberá protegerla mediante claves de acceso.

- Todos los empleados, contratistas y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no revelación).

ARTICULO NOVENO: CONTROL DE ACCESOS (DERECHOS Y RESPONSABILIDADES)

TIPOS DE USARIOS

Desde el punto de vista del tipo de conexión, los usuarios finales se denominarán:

- **Usuario Básico:** Aquel que puede acceder únicamente a los recursos de la Red e Internet; según los permisos dados por la Oficina de Planeación y Sistemas y/o administrador de la red.

- **Usuario Avanzado:** Aquel con capacidad de administrar los recursos del equipo y que además tiene acceso a los recursos de red e Internet. Este tipo de acceso implica responsabilidad total por ese dispositivo informático. Las limitaciones a estos servicios serán fijados por la Oficina de Planeación y Sistemas y/o administrador de la red.

- **Usuario Administrador.** Es aquel usuario o grupo de usuarios que tiene definidas funciones encaminadas a la administración los recursos físicos de la red y/o administrar el software centralizado de red (correo electrónico, antivirus, seguridad, etc.) y/o administrar los aplicativos críticos de gestión (nomina, inventarios, SIIF y otros)

Se define como Administrador de Red, a aquella persona o grupo de personas que tiene la responsabilidad de instalar o manejar los sistemas de red y los servidores y aplicativos del Centro de Computo de la Corporación.

RESTRICCIONES DE USO DEL INTERNET

Sin excepción, todos los usuarios de la red para la Cámara de Representantes, tienen restringido el acceso a páginas con contenido pornográfico, P2P (ares, limeware, emule, etc), Proxy Avoidance, Juegos, Tarjetas Postales, descargas de software Free.

- **Usuario Básico:** también será restringido el acceso a les redes sociales como Facebook, Twitter, Hi5, Messenger; Youtube, Skype entre otros. Con el fin de darle un mejor uso a este servicio y evitar su congestión, la entidad permitirá abrir el acceso a este tipo de páginas en el periodo comprendido entre lunes a viernes de 5:30 pm hasta 8:30 am.

- **Usuario Avanzado:** No tendrá restricciones del usuario básico, sin embargo se mantendrán las restricciones generales para todos los usuarios. Este usuario podrá ingresar sin restricción a todas los servicios de Internet y la intranet, a excepción de las restricciones generales ya establecidas.

- **Usuario Administrador.** Es un usuario VIP, no tiene ninguna restricción para el uso de los recursos de red, Internet e intranet; tan solo su accionar estará restringido a su rol que desempeña dentro de la Corporación.

NORMAS ESPECÍFICAS DE LOS USUARIOS

- **Representantes**
  Los Representantes que dispongan de recursos o dispositivos informáticos con conexión a Internet en sus oficinas o salones de sesiones, gozarán de acceso a todos los servicios de Internet y tendría privilegios de Usuario Avanzado. Son usuarios VIP, sin restricciones al uso de la Internet y la intranet; salvo las restricciones generales y las de acceso a los aplicativos críticos.

- **Funcionarios de Planta**
  Los funcionarios de planta, tendrán solamente privilegios de Usuario Básico. Quedan exceptuados aquellos, que por razones de manejo de aplicativos como de nomina KACTUS o de inventarios SEVEN o usuarios finales del Sistema Integrado de Información Financiera SIIF de Minhacienda o con labores muy específicas, deban tener privilegios especiales. En éste caso deberán contar con la aprobación del Jefe de la Oficina de Planeación y Sistemas previa solicitud y aprobación del jefe inmediato de la Dependencia a que le

corresponda. Específicamente podemos diferenciar los siguientes grupos de funcionarios:

Grupo SIIF. A este grupo de usuarios tienen perfiles bien definidos (consulta entidad, presupuesto, pagador, contable y registrador), los cuales le dan acceso a través de un router dotado por la Red de Alta velocidad del estado colombiano RAVEC, que por medio de un usuario y clave de acceso le da el acceso bien definido a los módulos del SIIF; sin embargo para acceder a la red, debe contar con un usuario que debe estar dentro del grupo de administradores locales de los computadores adscritos a los usuarios finales del SIIF, que previamente tanto el usuario como la terminal deben estar autenticados en el servidor de Minhacienda.

Grupo Kactus. Grupo que maneja el aplicativo de la nomina y recursos humanos; este grupo de usuarios debe estar bien definido para su autenticación en el servidor de aplicaciones en producción del centro de computo, en donde para poder ingresar debe contar con un usuario y un clave que debe ser idéntica a la configurada en el servidor o de lo contrario no lo dejaría ingresar, también debe tener derechos de administrador local de cada computador donde se accede. Como también, ya para el manejo interno del aplicativo debe contar con un usuario y una contraseña, dada por el administrador del aplicativo.

Grupo Seven. Grupo encargado del manejo del aplicativo de inventario y activos fijos; los usuarios deben estar configurados dentro del grupo de usuarios del servidor de aplicaciones en producción ubicado en el centro de computo, lo mismo que el usuario de acceso al equipo debe estar dentro del grupo de administradores locales de cada computador; como también debe contar con un usuario y clave que debe estar previamente configurado dentro del servidor donde se encuentre el aplicativo para poder ingresar, contando con clasificación de usuarios que permiten acceder específicamente a los módulos a que tengan privilegios.

- **Funcionarios Administrativos**

Los usuarios de recursos informáticos para uso administrativos solamente tendrán privilegios de Usuario Básico y salvo excepciones justificadas, se extenderán sus privilegios. El jefe de la Oficina de Planeación y Sistemas en concordancia con el administrador de red, podrá limitar el uso del equipo a aquellas aplicaciones administrativas directamente relacionadas con las funciones del usuario como empleado. Precisando un poco su rol especifico, podemos clasificarlos en:

Administrador de red. Se encarga de administrar todos los recursos físicos de la red, tales como: la administración del centro de computo, software de seguridad de red, software de servicios centralizados de red (directorio activo, correo electrónico, antivirus, continuidad del negocio – recuperación de desastres, agendación de visitas, sistema de gestión documental, entre otros).

Administrador de Aplicativos. Se encarga de la administración de usuarios y de los aplicativos críticos de la corporaciones, como son: Sistema Integrado de Información Financiera SIIF; Nomina y Recursos Humanos

KACTUS; Inventario y Activos fijos SEVEN; Consolidador de Hacienda e Información Financiera Publica CHIP.

- **Funcionarios UTL (Unidad de Trabajo Legislativo)**
  Los usuarios de UTL que es el grupo de trabajo compuesto hasta diez funcionarios con que cuenta cada Representante; tendrán los mismos privilegios de Usuario Básico.

DE LAS CUENTAS DE USUARIO

- El acceso a los servicios de la red serán administrados por la Oficina de Planeación y Sistemas en función de las necesidades y prioridades de la Corporación y de la disponibilidad de recursos.
- Se prohíbe la creación de cuentas anónimas o de invitado (guest). Toda cuenta establecida debe indicar claramente la identidad del usuario.
- Para la activación, bloqueo, expiración, cambio de privilegios o cancelación de un usuario por finalización de contrato, únicamente el Jefe de Dependencia podrá diligenciar un formato de solicitud al Jefe de la Oficina de Planeación y Sistemas.
- Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso.
- Las autorizaciones otorgadas a los usuarios para acceder a los recursos de la red son estrictamente individuales y no transferibles. Las mismas pueden expirar con el cese de las actividades que la han justificado o por la ausencia de renovación.
- Toda cuenta de usuario pedirá renovación de contraseña cada cuarenta y cinco (45) días.

CONTRASEÑAS

- El usuario no debe guardar su contraseña en una forma legible en archivos en su computador y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
- Deben crearse contraseñas de calidad empleando las siguientes reglas:
  - Sean fácil de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ej. nombres, números de teléfono, fecha de nacimiento, etc.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
  - Que contengan algún carácter especial.

- Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on"). En ese momento, el usuario debe escoger otra contraseña.
- No deben usarse contraseñas idénticas o substancialmente similares a contraseñas previamente empleadas.
- Verificar periódicamente, y cancelar IDs y cuentas de usuarios repetidos.
- No debe compartirse la contraseña o revelarla a otros. El hacerlo expone a las consecuencias por las acciones que los otros hagan con esa contraseña. Si hay razón para creer que una contraseña ha sido comprometida, debe solicitarse cambio inmediatamente.
- La contraseña asignada es personal e intransferible y esta bajo su directa responsabilidad.
- Esta prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadores, redes, y otros recursos del sistema. Para algún tipo de excepción de este ítem deberá ser solicitado directamente a la Oficina de Planeación y sistemas.
- Se limita a tres (3) el numero de intentos consecutivos infructuosos de introducción de la contraseña para lo cual la cuenta involucrada quedara automáticamente bloqueada.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la Cámara de Representantes.
- Si algún funcionario se ausenta por un lapso mayor a diez (10) días hábiles, el jefe inmediato debe informar a la Oficina de Planeación y sistemas.
- En temporada de vacaciones masivas, el Área de Recursos Humanos de la Honorable Cámara de Representantes debe enviar un listado vía mail al correo sistemas@camara.gov.co donde se enuncien los funcionarios que se ausentaran por este motivo, indicando la fecha de inicio y finalización de las mismas.

FINALIZACIÓN O TÉRMINO DEL CONTRATO DE EMPLEO

Retorno de activos informáticos

- Todos los empleados, deben retornar los activos de la Cámara de Representantes, que estén en su posesión hasta la finalización de su empleo, o contrato.
- El proceso de finalización debe ser formalizado para incluir el retorno previo de los recursos de software, documentos corporativos, y equipos. Otros activos de la corporación también han de ser devueltos.

Retiro de los derechos de acceso

- Los derechos de acceso para todos los empleados, a la información, y a las instalaciones del manejo de información o centros de cómputo deben ser removidos hasta la culminación del empleo.

Integridad y mantenimiento del Sistema
Los usuarios se comprometen a no interferir, voluntariamente, en el uso adecuado de los recursos de red. En particular:

- Está prohibida la modificación, de cualquier forma, a la estructura y topología de la red. En particular, está prohibido la remoción de recursos o dispositivos informáticos sin la autorización expresa, y por escrito del Jefe de la División de Planeación y Sistemas - administrador de la red.
- El usuario se compromete a no desarrollar, ni usar, aplicaciones que pudiesen poner en peligro la integridad y seguridad de la red.
- Los usuarios se comprometen a no reiniciar ningún recurso informático público, aún en aparente mal funcionamiento, sin autorización del Jefe de la División de Planeación y Sistemas - administrador de la red.
- Los usuarios se comprometen a no desconectar ningún recurso informático público, con la excepción de casos de emergencia, tales como fuego o peligro de choque eléctrico.

En caso de una emergencia, y en ausencia del Jefe de Planeación y Sistemas y/o administrador de la red, los usuarios podrán comunicarse directamente a la Oficina de Planeación y Sistemas o Mesa de Ayuda.

Acuerdos:
Tanto los usuarios Básicos como los Avanzados deben firmar un documento en el cual asume lo siguiente:

- El Usuario Avanzado se compromete, como Administrador del recurso o dispositivo informático, a no llevar a cabo operaciones que comprometan la integridad y seguridad de la red (por ejemplo: cambios de dirección IP, activación de servicios como DHCP, etc.)
- El usuario es el responsable por los servicios que presta el recurso informático asignado.
- El Usuario Avanzado se compromete a remitir, en sobre cerrado, al Jefe de Planeación y Sistemas y/o administrador de Red, la o las contraseñas de los recursos informáticos por los cuales es responsable, consintiendo, por ese medio, la intervención de la Oficina de Planeación y Sistemas, en caso de una emergencia.

ARTICULO DECIMO: SEGURIDAD FISICA Y DEL ENTORNO

Perímetro de seguridad física

- Se debe instalar sistemas adecuados de detección de intrusos de acuerdo a los estándares internacionales, y deben ser regularmente probados para cubrir todas las puertas externas y las ventanas de acceso, las áreas no ocupadas deben tener una alarma todo el tiempo, también se debe cubrir las áreas de salas de computo y cuartos de comunicaciones.

- Las áreas de cómputo y comunicaciones manejadas en la Cámara de Representantes, deben ser físicamente separadas de las manejadas por terceros.

Controles de acceso físico

- Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y salida deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados.

- El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas.

- Solamente el personal autorizado, miembro activo de la Oficina de Planeación y Sistemas es el único autorizado a tener acceso a los servidores de la unidad.

- Se debe requerir que todo el personal exhiba alguna forma de identificación visible.

- Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

- Los Administradores de Red deberán poseer todos los privilegios para monitorizar el correcto uso de los recursos de la red. En tal sentido, podrán analizar, sin que ello implique pérdida de los datos, todo el tráfico de un segmento, o de la totalidad de la red.

- En caso de un ataque por parte de un intruso, o en aquellos en que el correcto funcionamiento o la seguridad lo demande, el Administrador podrá revisar los archivos de un usuario y, en caso de infracción, podrá comunicarle sobre sus hallazgos al jefe de la Oficina de Planeación y Sistemas.

ARTICULO UNDECIMO: MARCO LEGAL.

Todo lo no contemplado en las presentes normas, queda sujeto a la legislación vigente sobre delitos informáticos y las instancias competentes. En caso que algún funcionario de la Cámara de Representantes incurra en alguna falta relacionada con las presentes políticas, se someterá en primera instancia a descargos con el Grupo de Control Interno Disciplinario y será juzgado por lo regulado por la siguiente legislación colombiana:

LEY 734 DE FEBRERO 5 DE 2002 CODIGO UNICO DISCIPLINARIO

Titulo IV, Capitulo Segundo, Artículo 34: Deberes. Son deberes de todo servidor público:

1. Cumplir y hacer que se cumplan los deberes contenidos en la constitución, los tratados de derecho internacional humanitario, los demás ratificados por el congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas, los contratos de trabajo y las ordenes superiores emitidas por funcionario competente.

Los deberes consignados en la ley 190 de 1995 se integran a este código.

4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado a la cual tenga acceso, e impedir o evitar las sustracción, destrucción, ocultamiento o utilización indebidos.

21. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente de conformidad con los fines a que han sido destinados.

22. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

24. Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.

25. Poner en conocimiento del superior los hechos que puedan perjudicar el funcionamiento de la administración y proponer las iniciativas que estime útiles para el mejoramiento del servicio.

Titulo IV, Capitulo Tercero, Articulo 35. Prohibiciones. A todo servidor público le esta prohibido:

1. Incumplir los deberes o abusar de los derechos o extralimitar las funciones contenidas en la constitución, los tratados internacionales ratificados en el congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas y los contratos de trabajo.

13. Ocasionar daño o dar lugar a la perdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder por razón de sus funciones.

21. Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas.

34. Proporcionar noticias o informes sobre asuntos de la administración, cuando no este facultado para hacerlo.

CODIGO PENAL

Todo servidor público, contratista o persona que preste servicios a la Honorable Cámara de Representantes y que incurrieren en la comisión de conductas que recaen sobre herramientas informáticas, llámese hardware y/o software, como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la reserva de la información, el patrimonio económico publico, la fe publica y la propiedad, le será aplicadas las normas que recoge el Código Penal para dichos delitos.

ARTICULO DUODECIMO: La presente Resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá a los

JAIRO JARAMILLO MATIZ
Director Administrativo

JESUS ALFONSO RODRIGUEZ CAMARGO
Secretario General

V/B. ANDREA DEL CARMEN CONTRERAS GONZALEZ, Jefe División Jurídica

Proyectó: **JESUS E. PINZON ORTIZ,** Jefe Oficina de Planeación y Sistemas