POLÍTICA DE USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI)
ARQUITECTURA EMPRESARIAL

Bogotá – Colombia
Marzo de 2021

INDICE DE CONTENIDO

1. INTRODUCCIÓN

El presente documento define las directrices y lineamientos para garantizar que todo el personal de la Cámara de Representantes, incluidas las partes interesadas, colaboradores, contratistas o terceros, den buen uso a los activos de información de la Cámara de Representantes.

2. OBJETIVOS

2.1. GENERAL

Establecer las especificaciones de seguridad para el uso aceptable de los activos de información.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

El presente documento tiene aplicabilidad a todos los colaboradores, contratistas o terceros a quienes se les haya otorgado permisos para realizar actividades sobre los activos de información de la Entidad.

4. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341	2009	Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1755	2015	Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II Capítulo I.
Conpes 3854	2016	Política Nacional de Seguridad Digital
Decreto 2364	2012	Firma electrónica
Decreto 2609	2012	Expediente electrónico Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693	2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

5. DEFINICIONES Y TÉRMINOS

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

Activos de Información: Es todo aquello que contiene, procesa, trate y/o manipule información valiosa para la Entidad y que son necesarios para que la Entidad funcione y cumpla con los objetivos establecidos para tal fin.

Acuerdo de Confidencialidad: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.

Administración: Conjunto ordenado y sistematizado de principios, técnicas y prácticas que tiene como finalidad apoyar el uso de la infraestructura de tecnología.

Autenticación: Asegurar que una característica declarada de una Entidad es correcta.

Autenticidad: Propiedad de que una Entidad es lo que dice ser.

Áreas seguras: Son todas aquellas instalaciones como centros de datos (principal y alterno), racks de comunicaciones de los puntos de atención y en cada piso de las sedes; en las que se realiza el procesamiento y envío de información del negocio. De igual forma, se consideran áreas seguras las que manejan información confidencial o privada.

Cifrado: Es el proceso que se aplica a unos datos para hacerlos incomprensibles. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de bits, de una medida determinada (longitud de clave). Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales y, por tanto, hacerlas otra vez comprensibles

Código Malicioso: El software malicioso es cualquier programa que busca deliberadamente causar un daño y/u obtener acceso no autorizado a los activos de información digital.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, Entidades o procesos no autorizados.

Configuración: La configuración es un conjunto de datos que determina el valor de algunas variables de un programa o sistema de software.

Controles: Medidas para que los riesgos sean reducidos a un nivel aceptable.

Dirección IP: Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.

Evidencia: Son los elementos probatorios que se consideran al momento de evaluar la culpabilidad o inocencia ante un incumplimiento de una política de seguridad de la información.

Hardware: Activos que representan toda la infraestructura física que permite el procesamiento, transporte y almacenamiento de información. Por ejemplo:

- Las Estaciones de Trabajo.
- Los equipos de comunicaciones, router, switch, firewall y cualquier otro elemento de una red de computadoras por donde transita la información.
- Los equipos portátiles.
- Los medios de almacenamiento.
- Los servidores.

Incidente de seguridad: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.

Información: Es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería,

comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.

Instalación: Añadir un programa de software a un computador.

Integridad: Propiedad de exactitud y completitud de la información.

Mantenimiento: Acciones necesarias para que un sistema tecnológico sea conservado de manera que pueda permanecer operando correctamente.

Medios: Se refiere a cualquier medio que contenga información, entre estos medios de almacenamiento, medios físicos como papel, entre otros.

Medios de almacenamiento de información: Son dispositivos para grabar o almacenar información (datos). Un dispositivo de almacenamiento puede guardar la información y procesarla. Dispositivos como los discos duros, CDs, memorias USB y algunas cintas de copia, son los medios de almacenamiento que generalmente se utilizan para almacenar información.

Medios removibles: Dispositivos tecnológico de almacenamiento de información diseñados para ser extraídos del computador.

Mejora Continua: El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El foco de la mejora continua es buscar oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas cómo podrían ser.

Monitoreo: Observar el curso de funcionamiento de un sistema para detectar posibles anomalías.

Operación: Se refiere a manejar los errores, manejar la trazabilidad en los registros de auditoría y la información del registro del sistema, procedimientos de inicio y apagado de los sistemas, las instrucciones específicas para procesar, manejar y proteger la información, y todos los procedimientos asociados con estas actividades.

Proceso: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

Política: Declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.

Red: Se refiere a los medios que permiten tele comunicar equipos de cómputo, y pueden ser internas y externas, y transmitir voz y datos. La red interna de la Entidad se conoce como LAN, la red externa para acceso de proveedores se conoce como EXTRANET, y la red que permite comunicación de la Entidad con el resto del mundo se conoce como INTERNET.

Riesgo: Es la probabilidad de que una amenaza se concrete sobre uno o más activos causando daños o perjuicios a la Entidad por medio de una vulnerabilidad o punto débil.

Seguridad de la información: Asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

Tecnología de la Información: Se refiere al hardware y software operados por la Entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Compañía, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotada por una a más amenazas.

6. DESCRIPCIÓN DE LA POLÍTICA

La Cámara de Representantes debe asegurar el uso adecuado de los activos de información de la Entidad, y velar por que todos los usuarios de la información conozcan y apliquen los lineamientos y controles que éste defina.

La Cámara de Representantes cuenta con diferentes tipos de activos de información y debe velar por el buen uso de éstos, a través de la definición y apropiación de los siguientes lineamientos:

6.1. LINEAMIENTOS DE USO DEL HARDWARE Y SOFTWARE

- Corresponde a la Oficina de Planeación 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 o en uso bajo cualquier modalidad de contratación, 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.
- No deben abrir o romper los sellos de seguridad instalados en cada computador por la Dirección Administrativa y Oficina de Planeación y Sistemas.
- No abrir, retirar o cambiar componentes de los equipos.
- Evitar prestar e intercambiar los equipos computacionales.
- Evitar instalar dispositivos o periféricos sin la supervisión y autorización expresa de la Oficina de Planeación y Sistemas.
- No retirar o sacar equipo de la institución sin previa autorización del área de almacén.

- Luego de adquirido el activo informático le corresponde a la Oficina de Planeación y Sistemas de la Cámara de Representantes las siguientes responsabilidades:
    - Implementar y velar por el cumplimento de las políticas, normas y procedimientos de seguridad y Privacidad de la Información de la Cámara de Representantes.
    - Estandarizar, formalizar y apropiar los procedimientos de seguridad, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro, eficiente y eficaz.
    - 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.
    - 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.
    - Elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática.
- 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.
- 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.
- 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.
- 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.
- 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.
- Se debe respetar la propiedad intelectual y licencias. El usuario no podrá copiar o redistribuir programas propiedad de la Honorable Cámara de Representantes.
- 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.

6.2. LINEAMIENTOS DE USO DEL CORREO ELECTRÓNICO

6.2.1. GENERALES

- El correo electrónico es un servicio de red para permitir a los usuarios de la Cámara de Representantes enviar y recibir mensajes para el desarrollo de sus funciones. En tal sentido, todos los usuarios del servicio deben asegurar el buen uso del recurso para garantizar la protección del servicio y de la información de la Entidad.
- El servicio de Correo debe usarse de manera responsable y exclusivamente para fines propios del desarrollo de las funciones y responsabilidades asignadas por la Entidad.
- Proteger el servicio de correo electrónico y los activos de información que pueden ser accedidos a través de éste, frente a las amenazas y vulnerabilidades identificadas de los resultados de la gestión de riesgos de seguridad digital, como la suplantación de identidad, el acceso no autorizado a información, indisponibilidad del servicio, y en general cualquier riesgo que afecte la disponibilidad, confidencialidad e integridad de la información.
- El acceso al servicio de correo electrónico debe ser autorizado por el responsable del proceso al que pertenece el funcionario, contratista o tercero que presta sus servicios a la Cámara de Representantes.
- Las cuentas de correo son personales e intransferibles y no se debe ceder el uso de la cuenta de correo a terceras personas, salvo en casos puntuales para los que deberá solicitarse y obtenerse la correspondiente autorización.
- Al finalizar su relación laboral todo funcionario, contratista o tercero que preste sus servicios a la Cámara de Representantes, debe realizar la devolución de la cuenta de usuario de correo electrónico al responsable del proceso para el cual laboraba, según los procedimientos establecidos.
- La clave de acceso al servicio de correo electrónico no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información la Cámara de Representantes.
- Controlar la difusión de las cuentas de correo, facilitando la dirección del correo electrónico sólo en los casos necesarios.
- Para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es conveniente utilizar contraseñas robustas, conforme a las políticas y lineamientos establecidos para tal fin.
- Evitar escribir correos a clientes o proveedores con información que pueda ser utilizada para comprometer a la Cámara de Representantes con algún tipo de información o acuerdo que no haya sido previamente autorizado.
- El uso del correo electrónico debe ser con el único propósito de realizar las labores específicas de la Cámara de Representantes.

- Debido a la importancia del correo electrónico como herramienta de comunicación dentro de la Cámara de Representantes, cada colaborador, contratista o tercero debe revisar su buzón de correo de forma continua durante su jornada laboral, a fin de asegurar que los mensajes se respondan a tiempo.
- Los sistemas de correo electrónico de la Cámara de Representantes deben ser utilizados únicamente para propósitos de las tareas asignadas y para el desempeño de sus obligaciones laborales.
- El usuario debe configurar las reglas en el servicio de correo electrónico debida a sus ausencias o, en su defecto, el responsable deberá realizar la solicitud para que se realice dicha configuración.
- Está prohibido utilizar cualquier sistema de correo diferente a los provistos por la Cámara de Representantes, para la ejecución de las funciones y responsabilidades que le fueron asignadas.
- Los sistemas de correo no aprobados o para fines diferentes a las funciones propias de la Cámara de Representantes, se consideran una fuente de riesgo para la información de la Entidad y, por lo tanto, está prohibido su uso.
- 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.
- Los siguientes usos del servicio de correo electrónico se consideran usos no autorizados y prohibidos los siguientes:
    - Envío de correos masivos sin autorización oficial.
    - Es estrictamente prohibido el envío de cadenas.
    - Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM
    - Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Entidad o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la entidad.
    - Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
    - Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
    - Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.

6.2.2. ENVÍO Y RECEPCIÓN DE CORREO ELECTRÓNICO

Todos los mensajes enviados desde los sistemas de correo de la Cámara de Representantes deben cumplir con los lineamientos de conformidad de la Entidad:

- Todos los mensajes enviados desde los sistemas de correo de la Cámara de Representantes deben cumplir con la legislación local y los instructivos de la Entidad.
- El asunto de la comunicación siempre debe ser indicado, como en cualquier correspondencia escrita. En el campo asunto del correo electrónico debe especificarse el nivel de clasificación de la información cuando ésta no sea pública, así como junto a la firma del correo. Esto asegurará que el correo se envíe protegido desde los sistemas de correo de la Cámara de Representantes.
- Los mensajes no deben ser leídos o enviados desde una cuenta de otro usuario, a excepción de los casos en que se hagan definiciones aprobadas para delegar a alguien por ausencia o retiro de una colaborador, contratista o tercero.
- Reemplazar, alterar, suplantar o producir cualquier falsa representación de la identidad de un usuario está prohibido (suplantación de direcciones).
- El correo electrónico es un recurso donde no se debe almacenar archivos de información importantes y por lo tanto los mensajes deben ser conservados sólo en la medida que sea necesario.
- Los usuarios de los correos electrónicos deben tener precaución cuando envían mensajes con información confidencial o restringida.
- Se debe evitar el envío de información a destinatarios erróneos, por lo cual los usuarios deben revisar los destinatarios del mensaje antes de proceder con su envío.
- El empleo de envío automático de mensajes con información rede este tipo por correo electrónico está prohibido si no se encuentra bajo el control de la Cámara de Representantes.
- El uso del correo electrónico está prohibido cuando se utilice para intercambiar información o software que violen las leyes de derechos de autor.
- El uso inapropiado de los recursos de correo electrónico puede exponer a la Cámara de Representantes a problemas de disponibilidad, por lo cual se debe establecer los límites para envío y recepción de correo, así como de espacio de almacenamiento.
- Los mensajes que contengan información confidencial en el cuerpo de correo o a través de un adjunto, deben ser clasificados y cifrados con el fin de proteger la confidencialidad de ésta.
- Los mensajes deben ser direccionados a receptores conocidos y necesarios.
- Los mensajes enviados innecesariamente pueden impactar el sistema y el desempeño del servicio de correo y, por ende, los usuarios del servicio deben asegurar que el uso de éste corresponde a las necesidades propias para el desarrollo de su función.
- El envío de correos a todos los miembros de un grupo de correo electrónico (listas de

distribución) está reservado para mensajes importantes y estrictamente necesarios.

- Las listas de distribución deben ser aprobadas por el Responsable de Seguridad de la Información de la Cámara de Representantes.
- Está prohibido, para cualquier usuario, originar o distribuir cualquier cadena de correo. Si estos mensajes son recibidos, debe notificarse inmediatamente al Responsable de Seguridad de la Información.
- La capacidad de almacenamiento del servicio de correo es limitada, por lo cual se debe conservar únicamente los mensajes que son imprescindibles y realizar actividades periódicas de depuración para aquellos mensajes que han quedado obsoletos.
- El uso aceptable del correo electrónico prohíbe la transmisión de los siguientes tipos de mensajes:
    - Ilegales y/o fraudulentos.
    - Difamatorios.
    - Ofensivos, obscenos, pornográficos, o de mal gusto.
    - Abusivos, bromistas o amenazantes.
    - Incitadores a infringir las Leyes.
    - Hostigamiento basado en sexo (acoso sexual), raza, nacionalidad, inhabilidades o cualquier otro.
    - Anónimos o mensajes repetidos diseñados para molestar o atormentar.
    - Mensajes que den opiniones políticas o sociales.
    - En los casos de recibir mensajes con dichas características deben ser informados inmediatamente al Responsable del Área y al Responsable de Seguridad de la Información de la Entidad, para su revisión, análisis, investigación o reportarse como un posible incidente de seguridad de la información.
- Se debe incluir en la cuenta de correo corporativo la información del “disclaimer” aprobado para el servicio de correo electrónico. Esta nota de confidencialidad ubicada al final del texto, después de la firma de éste, es una medida preventiva de divulgación no autorizada de contenidos a través del servicio correo electrónico. La nota de confidencialidad debe seguir el estándar definido por la Cámara de Representantes.

6.2.3. ARCHIVOS ADJUNTOS Y CONTENDIDOS EN LOS CORREOS ELECTRÓNICOS

- Enviar archivos en los correos es una de las formas más fáciles de transmitir un virus. Se debe tener cuidado para asegurar que los archivos recibidos son de una fuente confiable. Su contenido debe ser conocido antes de ser abierto o enviado.
- Los archivos recibidos serán chequeados automáticamente por el sistema, para verificar si contienen programas maliciosos. Si un correo electrónico tiene archivos con programas maliciosos, los archivos serán removidos automáticamente del correo.

- El emisor de un correo debe describir lo que contiene el(los) archivo(s) que anexa.
- El anuncio debe tener, al menos, la siguiente información:
    - Número de archivos.
    - Nombre y extensión de cada uno.
- No abrir archivos que se encuentren en correos electrónicos recibidos de remitentes desconocidos.

6.2.4. CONFIDENCIALIDAD

- La información confidencial o reservada no debe ser enviada por correo a través de redes públicas (por ejemplo, Internet) a menos que vaya protegida.
- En los casos en los que se requiera envío o recepción de información pública clasificada con carácter reservado, el usuario del servicio de correo electrónico debe cifrar dicha información, de acuerdo con las políticas establecidas.
- Se debe garantizar que la información se protege adecuadamente al ser enviada por el servicio de correo electrónico corporativo, para lo cual se debe escribir en el asunto del correo la clasificación de la información que está enviando.

6.2.5. REENVÍO DE CORREO ELECTRÓNICO

- El reenvío de mensajes con información confidencial o restringida está prohibido.
- La información enviada por correo electrónico por defecto está clasificada como interna. Los usuarios deben tener cuidado al reenviar mensajes, debido a que puede no ser apropiado distribuirlos.
- El uso de reglas que permitan reenviar de manera automática correos electrónicos a direcciones que no sean de la Cámara de Representantes (direcciones externas2) está prohibido.
- Cuando se responde o reenvía un mensaje se deben revisar las direcciones de correo a las cuales se va a remitir dicha respuesta o reenvío. Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido

6.2.6. FIRMA DE CORREO SALIENTE

- Todo correo enviado a través de los sistemas de correo de la Cámara de Representantes debe tener obligatoriamente la firma del funcionario, donde se incluyan al menos los siguientes datos:
    - Nombre completo.
    - Cargo.
    - Área.

- Teléfono y extensión.
- Dirección de correo electrónico.
- Dirección de la oficina del empleado.
- Dirección de la página Web de la Cámara de Representantes.

6.2.7. MONITOREO, REGISTRO E INTERCEPTACIÓN

- La Cámara de Representantes se reserva el derecho de monitorear o interceptar cualquier tráfico de correo electrónico como parte de sus actividades operacionales, de acuerdo con la legislación colombiana.
- Los mensajes entrantes y salientes pueden ser monitoreados como parte del monitoreo de desempeño de los sistemas, mantenimiento, investigación, auditoría o actividades relacionadas con seguridad. Esto es necesario para asegurar que los colaboradores utilizan adecuadamente el correo electrónico y que cumplen con las políticas internas establecidas.
- El tráfico de correo puede ser registrado por las razones dispuestas en el numeral anterior.
- Implementar herramientas de monitoreo y registros de auditoría no da derecho a los administradores de los sistemas, ni a los responsables de áreas para ver el correo de los colaboradores a menos que exista una investigación en curso u orden judicial explícita y bajo los procedimientos internos y judiciales aplicables.

6.2.8. BORRADO / RETENCIÓN DE CORREO ELECTRÓNICO

- Los sistemas de correo no pueden garantizar almacenamiento por largo tiempo, ni completo borrado de los mensajes. Por esto se hace necesario que cada usuario tenga configuradas y utilice carpetas en Drive o en el repositorio autorizado para tal fin, de esta manera se asegura que cualquier problema en el servidor de correo no ocasionará pérdidas de información a los usuarios.

6.2.9. ACCESO REMOTO AL SERVICIO DE CORREO ELECTRÓNICO

Los usuarios del servicio de correo electrónico de la Cámara de representantes, deben adoptar los siguientes lineamientos para acceder de forma remota al servicio:

- Los navegadores utilizados para acceder al servicio de correo deben estar permanentemente actualizados a su última versión y correctamente configurados.
- Se debe mantener desactivadas las características de recordar contraseñas para el navegador, y en los casos que no sea posible, los usuarios no deben guardar las credenciales de acceso al servicio de correo electrónico en el navegador.
- Se debe realizar la desconexión con el servidor de correo electrónico y/o la finalización de la sesión hacia el servicio a través de los procedimientos adecuados, con el fin de evitar la reutilización de la sesión

- Está prohibida la instalación de complementos en el navegador, salvo autorización explícita para ello.
- Se debe activar el borrado automático de la información de la actividad realizada y registrada por el navegador cuando se cierra éste.

6.2.10. TRATAMIENTO DE CUENTAS DE CORREO ELECTRÓNICO CUANDO UN COLABORADOR SE RETIRA

- Cuando se recibe la confirmación de retiro de un colaborador, se debe iniciar el proceso de creación de alias para el superior jerárquico, con el fin de tener una trazabilidad de los correos que se reciben después del retiro.
- Se deberá realizar una copia de respaldo para la cuenta y almacenarla según lo establecido en la Política de Respaldo de la Cámara de Representantes.
- Se debe contar con los procedimientos e instructivos necesarios para el restablecimiento de las cuentas que hayan sido eliminadas y que sea necesaria su recuperación.
- El superior jerárquico debe definir el tiempo de retención de dicha información o quedar como responsable de la misma, según los intereses y necesidades del área.

6.2.11. CUENTAS DE CORREO ELECTRÓNICO INACTIVAS

- Periódicamente se debe realizar la revisión de las cuentas que llevan más de 60 días sin ningún acceso, en caso tal, se procederá a enviar una comunicación de las cuentas sin uso al propietario de la cuenta y/o al responsable superior inmediato para obtener respuesta de la actividad de la misma y se darán 30 días adicionales a partir de la fecha de la comunicación para la utilización de la cuenta. Vencidos los treinta días, de no presentarse uso y/o respuesta del responsable superior inmediato, se procederá a su eliminación y se entenderá que el usuario ya ha sido comunicado y se tomaran las medidas necesarias para hacer uso de la licencia.

6.2.12. USO DE CORREO ELECTRÓNICO PERSONAL

- Los usuarios de la Cámara de Representantes podrán hacer uso del correo electrónico, siempre y cuando ello no vaya en detrimento ni incumplimiento de sus funciones laborales, ni afecte la operatividad de los sistemas informáticos de la Entidad.
- El uso del correo electrónico personal se realiza bajo la responsabilidad propia de cada usuario y únicamente para su uso personal.
- Está prohibido el uso del correo electrónico personal para el envío o la recepción de cualquier tipo de información o de los procesos propios de la Cámara de Representantes.
- Está prohibido el uso del correo electrónico personal, si éste pone en riesgo los activos de información de la Entidad.

- Los lineamientos y buenas prácticas definidos en la presente política y en los procedimientos e instructivos definidos por la Cámara de Representantes, aplican para el uso y/o acceso al correo electrónico personal, a fin de proteger los activos de información de la Entidad.

6.3. LINEAMIENTOS DE USO DEL SERVICIO DE INTERNET

Se deben adoptar las medidas necesarias para propiciar el correcto uso del servicio de Internet, con el propósito de minimizar los riesgos para la Cámara de Representantes, derivados de su uso.

6.3.1. GENERALES

- El servicio de Internet debe usarse de manera responsable y exclusivamente para fines propios del desarrollo de las funciones y responsabilidades asignadas por la Entidad.
- No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o puede llegar a atentar contra la dignidad humana. Así mismo, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.
- No visitar páginas no fiables o sospechosas con el fin de evitar posibles incidentes de seguridad y privacidad de la información.
- Cuidar la información que se publica en Internet. No se debe proporcionar información sobre la Cámara de representantes en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta.
- No debe enviarse a través de Internet mensajes con información confidencial a menos que tal información esté cifrada.
- Está prohibido difundir sin autorización cualquier tipo de información no pública sobre la Entidad, sus recursos, sus activos de información, los datos personales, su funcionamiento interno, etc.
- Antes de utilizar una información obtenida de internet, Los usuarios deberán comprobar los derechos de la Propiedad Intelectual o Industrial de la información obtenida de internet.
- Todo usuario es responsable de las acciones efectuadas a través de este servicio, tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red la Cámara de Representantes o se reciba desde Internet empleando la cuenta de acceso que se le ha suministrado.
- Cuando un funcionario o contratista al que le haya sido autorizado el uso de una cuenta servicio de Internet o de acceso a la red local de la Entidad finalice su vinculación con la Entidad, deberá seguir los procedimientos definidos por la Entidad para entregar su cuenta de usuario y accesos a servicios informáticos provistos por la Entidad.
- Se debe filtrar todo contenido que vaya en contra del interés de la Cámara de Representantes.

- El uso aceptable de Internet prohíbe el acceso a sitios que contengan mensajes:
    - Ilegales y/o fraudulentos.
    - Difamatorios.
    - Ofensivos, obscenos, pornográficos, o de mal gusto.
    - Abusivos, bromistas o amenazantes.
    - Incitadores a infringir las Leyes.
    - Hostigamiento basado en sexo (acoso sexual), raza, nacionalidad, inhabilidades o cualquier otro está prohibido.
    - Anónimos o diseñados para molestar o atormentar.
    - Sitios de opinión política o social.

6.3.2. ACCESO A LOS SERVICIOS DE INTERNET

- La Cámara de Representantes otorgará acceso a internet, siempre que se estime necesario para la ejecución de las funciones de los colaboradores y cuando exista disponibilidad para ello.
- El uso de Internet es personal e intransferible no permitiéndose que terceras personas hagan uso del servicio.
- Se debe garantizar que el acceso al servicio de internet por parte de personal externo y que se encuentre dentro de las instalaciones de la Entidad se encuentra configurado en segmentos totalmente independientes a los segmentos de red, para evitar accesos no autorizados a la información.
- Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en la Cámara de Representantes y para los cuales este formal y expresamente autorizado.
- Todo usuario es responsable de informar si cuenta con acceso a contenidos o servicios que no le estén autorizados o no correspondan a sus funciones dentro la Cámara de Representantes.
- El uso personal de Internet se permite de acuerdo con límites razonables, mientras los sitios visitados no sean ilegales o inapropiados al ambiente de trabajo (por ejemplo, pornografía, juegos, armas, entre otros tipos de sitios).
- Se prohíbe el acceso a los recursos de internet que puedan colocar en riesgo los activos de información de la Cámara de Representantes.
- El servicio de Internet no debe ser utilizado para violar la propiedad intelectual de otras personas. La propiedad intelectual incluye derechos de autor, marcas registradas, imágenes, fotos, videos, software, investigaciones firmadas, patentes, secretos de mercadeo, publicidad, etc. Los colaboradores tienen prohibido interferir o atentar contra las medidas de derechos de autor implementadas para proteger la información

o identificar los trabajos de los dueños.

- La Cámara de Representantes se reserva el derecho de bloquear el acceso a los sitios que considere inapropiados. El acceso intencional y continuo a estos sitios resultará en sanciones disciplinarias.
- 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 y/o de la mesa de ayuda.
- 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.

6.3.3. DESCARGA DE PROGRAMAS

- La descarga de archivos de Internet (especialmente ejecutables, pero también otro tipo de archivos) está prohibida, si no hace parte de funciones y actividades propias de su trabajo.
- Todas las descargas de Internet automáticamente serán chequeadas contra virus en la estación de trabajo local. Si alguno de los archivos está infectado con virus, el empleado debe reportarlo inmediatamente a la Mesa de Servicio.
- La Cámara de Representantes se reserva el derecho de bloquear otros tipos de archivos que considere inapropiados. El acceso intencional y continuo a este tipo de archivos resultará en sanciones disciplinarias.
- No se debe descargar, instalar, copiar o almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor o que generen algún riesgo para la Entidad.
- No se debe descargar, instalar, copiar o almacenar programas computacionales, software y demás materiales electrónicos desconocidos o no confiables, sin asegurar la confiabilidad del sitio y utilizando las páginas oficiales para ello. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas.
- La transferencia (descarga) de archivos electrónicos de Internet está prohibida, a menos que sea como parte necesaria para el desarrollo de sus funciones.

6.3.4. USO PARA LOS OBJETIVOS PROPIOS DE LA ENTIDAD

- Todo el uso de Internet debe ser apropiado a los propósitos de los objetivos de la Cámara de Representantes y debe tener en cuenta los requisitos para la protección de la confidencialidad e integridad de la información.
- Los colaboradores tienen prohibido interferir o tratar de deshabilitar mecanismos antipiratería u otras medidas técnicas de protección utilizadas por los dueños de los derechos de propiedad para proteger o identificar su trabajo (por ejemplo, software).

- Tener acceso a otros recursos en Internet más allá de la Web está reservado a los usuarios autorizados de los sistemas, se debe limitar a los propósitos legítimos, y debe ser conforme con la legislación y a las políticas de la Cámara de Representantes.
- Cualquier tipo de ataque, así como efectuar un escaneo, prueba o penetración de sistemas de computación o redes en Internet, o redes internas, está estrictamente prohibido. Cualquier ataque o prueba detectada y que haya sido realizada por un colaborador, implicará sanciones disciplinarias.

6.3.5. PUBLICACIÓN EXTERNA

- Los colaboradores no deben colocar artículos o comentarios sobre la Entidad en grupos de noticias, blogs, o páginas que permitan estos servicios, sin autorización previa del área de comunicaciones de la Cámara de Representantes.
- Está prohibido publicar en Internet información interna, confidencial o restringida de la Cámara de Representantes.

6.3.6. MONITOREO

- La Cámara de Representantes se reserva el derecho de efectuar registro, monitoreo o interceptación del acceso a Internet como parte de sus actividades operativas normales, dentro del marco de la legislación colombiana.
- La Cámara de Representantes se reserva el derecho de monitorear o interceptar cualquier tráfico desde y hacia internet como parte de sus actividades operacionales, de acuerdo con la legislación colombiana.
- El tráfico entrante y salientes pueden ser controlado como parte del monitoreo de desempeño de los sistemas, mantenimiento, investigación, auditoría o actividades relacionadas con seguridad y privacidad de la información.
- El tráfico de correo puede ser registrado por las razones dispuestas en el numeral anterior.

6.4. LINEAMIENTOS DE USO DE LOS SERVICIOS DE RED

6.4.1. DISPOSITIVOS DE USUARIO FINAL

- Los usuarios no deben conectar ningún dispositivo (por ejemplo, equipo portátil, teléfonos celulares) directamente a la red interna, a menos que el dispositivo haya sido aprobado por el responsable de Seguridad de la Información.
- El almacenamiento de información interna, confidencial o restringida en dispositivos debe ser autorizado previamente por el dueño de la información. Está prohibido el almacenamiento de información en dispositivos personales, salvo previa autorización del responsable de la información y según la valoración de los riesgos.
- Si un dispositivo conectado a la red interna es utilizado por personal externo, debe

existir un contrato validado por el Responsable de la Oficina Jurídica de la Cámara de Representantes con el colaborador o con el tercero que incluya cláusula de confidencialidad y de cumplimiento de las políticas de seguridad y privacidad de la información de la Cámara de Representantes. El colaborador (externo) se debe someter a todas las políticas y instructivos de seguridad de la Cámara de Representantes, así como a las políticas específicas de seguridad que existan para las redes y los sistemas usados.

- Antes de permitir el acceso a la red interna, el área de la Cámara de Representantes responsable por la relación contractual con el colaborador, contratista o tercero debe verificar que todos los acuerdos necesarios estén firmados.
- Cualquier información almacenada en dispositivos personales debe ser borrada si así lo requiere o si el empleado deja la Entidad.

6.4.2. DATOS DE CONFIGURACIÓN DE LA RED

- Ningún usuario de la Cámara de Representantes o externo, que se encuentre utilizando un equipo de cómputo conectado a la red interna, deberá modificar o intentar realizar algún cambio no autorizado de los datos de identificación del equipo (por ejemplo, nombre en la red, grupo de trabajo o dominio, dirección IP, etc.) que le han sido asignados.
- 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. En situaciones de emergencia se deben seguir los procedimientos preestablecidos y aprobados por la Entidad. Todo esto es para evitar problemas por cambios no planificados que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.
- Los cambios sólo pueden ser realizados por el personal autorizado para este fin. Cualquier problema que se genere en la red de la Cámara de Representantes debido a un cambio no autorizado en los datos de configuración, en cualquier equipo, ocasionará sanciones disciplinarias.
- Los privilegios especiales, de posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de los sistemas.
- Se debe ejercer gobierno, control y protección de los accesos privilegiados a los activos de información de la Cámara de Representantes, como mínimo en aquellos considerados como críticos o fundamentales para los procesos y los servicios de la Entidad.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados de manera periódica y como mínimo semestralmente. La Oficina de Planeación y Sistemas debe revocar los privilegios de un usuario cuando reciba una orden de un superior, y en

particular cuando un empleado cesa en sus funciones.

- Cuando un empleado se retira de la Cámara de Representantes, la División de Personal debe informar de inmediato a la Oficina de Planeación y Sistemas para que se desactive la(s) cuenta(s) de usuario asignada(s).

6.4.3. CONEXIONES A INTERNET

- Está prohibido que los usuarios conecten equipos de comunicaciones en la red corporativa o en sus equipos de cómputo para conectarse directamente a Internet.
- Los equipos que tengan instalados dispositivos de comunicación no autorizados deben ser reportados a la Mesa de Servicio para que se realicen los procesos establecidos por la Entidad.
- Los colaboradores que tengan este tipo de equipos de comunicación previamente autorizados no deben conectarse a Internet u otra red externa mientras el computador esté conectado a la red interna de la Cámara de Representantes.
- Cualquier incidente de seguridad generado por una conexión no autorizada, acarreará sanciones disciplinarias para el usuario.

6.4.4. SITIO WEB DE LA CÁMARA DE REPRESENTANTES

- Si algún empleado se da cuenta de incidentes con páginas Web de los sitios de la Cámara de Representantes, debe informar inmediatamente al Oficial de Seguridad de la Información.

6.5. LINEAMIENTOS DE USO DE LOS EQUIPOS DE CÓMPUTO

6.5.1. GENERALES

- Los computadores, cuentas de usuario, teléfonos (incluyendo los celulares), buzones de correo de voz y otros recursos similares que son propiedad de la Cámara de Representantes, son asignados para asistir a sus colaboradores en el desempeño de su trabajo diario.
- La Cámara de Representantes se reserva el derecho de acceso a todos los equipos usados para desempeñar los objetivos de la Cámara de Representantes, incluyendo cualquier dispositivo que procese, utilice, almacena, transmite información.
- La información y equipos de la Cámara de Representantes que son utilizados fuera de la oficina siguen siendo propiedad de la Cámara de Representantes. Los equipos son solamente para tareas autorizadas por parte de la Cámara de Representantes y en ningún momento para efectos personales. La información y los equipos que son sacados fuera de la oficina deben ser protegidos por los colaboradores como si estuvieran en la oficina.
- Todos los recursos de tecnología provistos por la Cámara de Representantes son para uso de los objetivos de la Cámara de Representantes únicamente. Utilizar los recursos

de la Cámara de Representantes para realizar otras tareas que no concuerden con la labor asignada no está permitido.

- Los recursos de tecnología provistos por la Cámara de Representantes no deben ser utilizados para jugar, aunque los juegos sean provistos por el sistema operativo.

6.5.2. EQUIPOS PORTÁTILES

- Los equipos portátiles son especialmente sensibles a robo o pérdida y requieren unas medidas de seguridad más altas. En ningún momento se deben dejar descuidados en sitios públicos.
- Cuando se encuentren instalados en su puesto de trabajo, siempre deben estar asegurados con la guaya de seguridad entregada para tal fin y para las guayas con clave numérica, ésta nunca debe ser dejada incluso al retirar el portátil de la guaya.
- Los cables de conexión a la corriente no están siendo estirados, mordidos, roídos o colocados de una manera que se considere riesgosa.
- Los ventiladores y las grillas no estén siendo obstruidos.

6.5.3. ACCESO A LOS EQUIPOS DE CÓMPUTO

- Todo el personal de la Cámara de Representantes, incluyendo a funcionarios, contratistas y terceros que interactúan con la información de la Entidad deben apropiar la **Política de Gestión de Acceos** definida como parte de la **Política General de Seguridad y Privacidad de la Información**.
- Los colaboradores deben asegurarse en el momento en que dejen su puesto de trabajo u oficina, que sus computadores estén apagados o bloqueados.
- Se debe tener configurado el protector de pantalla en los equipos de cómputo luego de un tiempo determinado. Este protector debe estar protegido con contraseña. Por ningún motivo los usuarios deben deshabilitar el protector de pantalla, la protección de contraseña de éste, o cambiar el tiempo de activación del protector de pantalla a un tiempo mayor al establecido. Si por algún motivo, algún usuario no tiene esta configuración en su computador, o cree que no funciona adecuadamente, deberá solicitar su revisión y/o configuración a la Mesa de Servicio.
- Los equipos de cómputo deben tener configurado el acceso por credenciales al inicio del sistema, para iniciar o restablecer la sesión y, cuando se considere necesario, al arranque del sistema operativo. Estas características no deben ser deshabilitadas.

6.5.4. ALMACENAMIENTO DE DATOS

- Los equipos portátiles no deben almacenar información confidencial o restringida si esta no se encuentra adecuadamente protegida.
- Los usuarios que almacenen información confidencial o restringida de la Cámara de Representantes en el equipo de cómputo asignado deben realizar una copia de

seguridad de la información para asegurar su disponibilidad. Para ello puede solicitar a la Mesa de Servicio la realización de una copia de seguridad (backup) de la información o realizarla de manera individual mediante los procedimientos y recursos aprobados por la Entidad.

- Está prohibido el almacenamiento de la información de la Cámara de Representantes en recursos diferentes a los autorizados para este propósito.
- La información confidencial o restringida que deba ser almacenada en medios diferentes al computador autorizados por la Entidad (por ejemplo, CDs, memorias USB, DVD, Almacenamiento en Nube, etc.) debe:
    - Estar protegida contra acceso no autorizado.
    - Utilizar los medios de almacenamiento autorizados pos la Entidad.
    - Emplear mecanismos de cifrado de la información para impedir la pérdida de la confidencialidad o de la integridad de ésta.
    - Borrar y formatear los dispositivos de almacenamiento electrónico autorizados, antes de realizar el copiado de la información.
    - Realizar, a través de los procedimientos adecuados y autorizados, el borrado seguro de la información.
- Los medios de almacenamiento electrónico de datos y los medios físicos como el papel, que tengan información confidencial o restringida, deben ser físicamente destruidos antes de ser arrojados a la basura. El papel impreso con información confidencial o restringida nunca debe ser reutilizado.

6.5.5. TRANSPORTE

- Si los equipos portátiles son transportados en un automóvil, estos no deben ser dejados en un sitio que sea visible.
- Durante el transporte, el equipo portátil debe ser guardado adecuadamente, de manera que no se caiga en caso de accidente.

6.5.6. SEGURIDAD DE TELÉFONOS

- Los colaboradores deben tener cuidado al transmitir información por teléfono, ya que éste medio no es seguro y puede ser interceptada por personas no autorizadas.
- Cuando se dejen mensajes de voz en buzones, para cualquier colaborador, contratista o tercero, conteniendo información confidencial, los colaboradores deben afirmar, al principio del mensaje, que la información que se está dejando es confidencial o restringida.
- Mensajes con información confidencial o restringida no deben ser dejados con otras personas.

6.6. LINEAMIENTOS DE USO DE INFORMACIÓN IMPRESA

6.6.1. GENERALES

- El material impreso producido utilizando los recursos de tecnología de la Cámara de Representantes debe ser tratado con la misma precaución con la que se manejan los datos almacenados electrónicamente. Todo el material impreso debe ser tratado de acuerdo con los lineamientos de seguridad establecidos por la Cámara de Representantes.
- El envío de material impreso que contenga información confidencial o estrictamente confidencial, a través de correo físico, debe ser enviado con las medidas necesarias para garantizar su protección, confidencialidad e integridad y emplear sobre sellado marcado con una etiqueta que lo distinga y que indique que es “sólo para el destinatario”.
- Cuando se requiera el envío de información confidencial o restringida de la Entidad, se deben utilizar servicios que permitan realizar seguimiento y trazabilidad del material enviado como los servicios de correo certificado.
- Para prevenir cualquier lectura no autorizada o búsqueda de información, en dispositivos de reproducción de información como impresoras, fotocopiadoras, multifuncionales, entre otras, no se debe dejar abandonado el material impreso.
- Los documentos que contienen información sensible se deben retirar de las impresoras inmediatamente.
- Todo el material impreso que no sea retirado de los dispositivos de reproducción podrá ser destruido.

6.6.2. DESTRUCCIÓN DEL MATERIAL IMPRESO

- El material impreso con información interna, confidencial o restringida debe ser destruido utilizando una máquina de destrucción de papel, o debe romperse en varios pedazos y, en todo caso, debe distribuirse en diferentes depósitos de papel.
- Por ningún motivo material con información interna, confidencial o restringida debe ser reutilizado.

6.6.3. SEGURIDAD AL ESCANEAR IMÁGENES

- El equipo de trabajo que sea responsable por, o que utilice los escáneres de imágenes, debe asegurar que el contenido del material escaneado es mantenido sólo para propósitos de los objetivos de la Cámara de Representantes.
- Asegurar que los derechos de autor del material origen no sean violados. Cuando ya no se necesite, el material escaneado debe ser eliminado del equipo. El material Confidencial o restringido que sea escaneado debe ser almacenado de manera segura, no debe ser compartido en carpetas.

6.7. LINEAMIENTOS USO INACEPTABLE

Los siguientes son prácticas indebidas o inapropiadas, por lo cual son prohibidas o inaceptables:

- Acceso no autorizado a sistemas de cómputo o redes.
- Violación de los derechos de privacidad de terceras partes.
- Violación a los derechos de propiedad intelectual de terceras partes.
- Transmisión de amenazas, material obsceno o de hostigamiento.
- Transmisión ilegal de publicidad no solicitada.
- Corrupción o destrucción de datos o cualquier acción que pueda impedir el acceso legítimo a los datos, incluyendo la carga de un virus, de gusanos o de cualquier software dañino en cualquier sistema de cómputo conectado a la red.
- Interrupción del uso legítimo de la red o de un sistema de cómputo por terceras partes.
- Desperdicio de los recursos de la red.
- Cualquier uso condenado por las políticas de uso aceptable de la red conectada.
- Cualquier conducta ilegal de contrato con la legislación aplicable de cualquier país al que se pueda tener acceso por la red.
- Uso de la red para juegos recreativos.
- Uso comercial de la red.
- Uso de la red para transmisión de publicidad comercial

6.8. OTROS LINEAMIENTOS

- El uso de los recursos de tecnología para propósitos ilegales o propósitos inapropiados para el ambiente de trabajo está estrictamente prohibido y puede resultar en acciones disciplinarias.
- Todo el personal de la Cámara de Representantes, incluyendo a funcionarios, contratistas y terceros que interactúan con la información de la Entidad deben apropiar la **Política de Escritorio Limpio y Pantalla Limpia** definida como parte de la **Política General de Seguridad y Privacidad de la Información**.
- Todos los colaboradores partes interesadas, terceros deben cumplir la **Política de Seguridad y Privacidad de la Información** de la Entidad y debe apropiar los lineamientos y buenas prácticas definidas para el aseguramiento y la protección de la información.

7. RESPONSABLES

- **Responsable de Seguridad de la Información**: Velar por el cumplimiento de la presente política para garantizar el desarrollo continuo de las capacidades de la Cámara de Representantes para responder a los incidentes de seguridad de la información y seguridad digital.
- **Responsable de la Oficina de Planeación y Sistemas**: Disponer de los recursos necesarios para el cumplimiento de los lineamientos descritos en la presente política.

8. INCUMPLIMIENTO

El incumplimiento de la Política de Uso Aceptable de Activos de Información de la Entidad podrá constituir falta disciplinaria y será sancionada en el marco del Código Disciplinario Único – Ley 734 de 2002.

9. REFERENCIAS

- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información – 2016.
- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información, *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información - 2016.*
- International Organization for Standardization, ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems.

10. CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
1	16/12/2021	• 03/11/2020 Creación del Documento. • 30/11/2020 Ajuste del Formato. • 12/03/2021 Se incluyen los numerales 6.2.10 y 6.2.11 referentes a cuentas de colaboradores retirados y cuentas inactivas.	Oficina de Planeación y Sistemas Ing. Elgar Castillo Rueda – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Ing. Sebastián Del Toro Montalvo Ing. Álvaro Carreño Ortiz Aprobación: Comité Institucional de Gestión y Desempeño 16/12/2021.