**CÁMARA DE REPRESENTANTES**



**MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA CÁMARA DE REPRESENTANTES V2.0**

**JULIO DE 2020**

TABLA DE CONTENIDO

[1. INTRODUCCION 3](#_Toc44582625)

[2. OBJETIVOS 4](#_Toc44582626)

[2.1 OBJETIVO GENERAL 4](#_Toc44582627)

[2.2 OBJETIVOS ESPECÍFICOS 4](#_Toc44582628)

[3. ALCANCE 5](#_Toc44582629)

[4. POLÍTICAS GENERALES DE SEGURIDAD TECNOLÓGICA DE LA CÁMARA DE REPRESENTANTES 6](#_Toc44582630)

[5. POLÍTICA DE USO DE SERVICIO DE ACCESO A INTERNET 8](#_Toc44582631)

[6. POLÍTICA DE USO DE SERVICIOS DE CORREO ELECTRÓNICO 11](#_Toc44582632)

[7. POLÍTICA DE RESPALDO DE INFORMACIÓN 13](#_Toc44582633)

[8. POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN 14](#_Toc44582634)

[9. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN 16](#_Toc44582635)

[10. POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES 17](#_Toc44582636)

[11. POLÍTICAS DE SEGURIDAD PARA CONTRASEÑAS Y EL CONTROL DE ACCESO 18](#_Toc44582637)

[11.1 IDENTIFICACIÓN DE EQUIPOS EN LA RED 20](#_Toc44582638)

[11.2 SEGREGACIÓN EN REDES 20](#_Toc44582639)

[11.3 CONTROL DE CONEXIONES A LA RED 21](#_Toc44582640)

[11.4 CONTROLES DE ROUTING DE LA RED 21](#_Toc44582641)

[11.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS 21](#_Toc44582642)

[11.6 CIERRE DE UNA SESIÓN DE RED POR INACTIVIDAD 22](#_Toc44582643)

[12. POLÍTICAS DE ADMINISTRACION DE HARDWARE Y SOFTWARE 22](#_Toc44582644)

[13. POLÍTICAS DE SEGURIDAD PARA REDES 24](#_Toc44582645)

[14. POLÍTICA DE TELETRABAJO 25](#_Toc44582646)

[15. POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE 26](#_Toc44582647)

[16. TIPOS DE FALTAS 28](#_Toc44582648)

[17. TERMINOS Y DEFINICIONES 30](#_Toc44582649)

[18. RESPONSABLE DEL DOCUMENTO 34](#_Toc44582650)

**MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA**

**CÁMARA DE REPRESENTANTES**

# INTRODUCCION

Este documento actualiza al Manual de políticas de seguridad de la información adoptado por la Resol.1405 de 2019 de la Entidad.

La Cámara de Representantes estipula que la información es de gran importancia para la misma ya que de ella emanan las acciones misionales que le fueron encargadas por la constitución política y la ley, por tal motivo se generan medidas para su protección y confidencialidad, en razón a esto se definen políticas de seguridad de la información, que son mecanismos administrativos de control de los riesgos y tienen como objetivo definir los requisitos para preservar la confidencialidad, integridad y disponibilidad de la información de la Entidad frente a potenciales amenazas. Las políticas son lineamientos generales que se traducen en procedimientos y controles debidamente alineados a las necesidades y objetivos estratégicos de la Entidad.

Es de tener en cuenta que el incumplimiento de las políticas de seguridad de la información puede conducir a riesgos que derivan en pérdidas de confidencialidad, integridad o disponibilidad de la información y en casos extremos a incidentes de seguridad de la información que dependiendo de su severidad conducen a procesos administrativos, disciplinarios o legales según el impacto del evento de seguridad provocado.

Para la Entidad los recursos de tecnológicos son considerados un activo valioso que debe ser aprovechado y utilizado en beneficio de la operación y eficiencia de la Entidad, por lo tanto las políticas establecidas en el presente documento deben ser de estricto cumplimiento para cada uno de los funcionarios, contratistas y/o visitantes de la Entidad que en ejercicio de sus funciones accedan o hagan uso la infraestructura y demás recursos tecnológicos de la Honorable Cámara de Representantes. Este documento se encuentra enfocado en las buenas prácticas de seguridad de la información, la estrategia de Gobierno en Digital en los lineamientos de la norma técnica ISO 27001/2013.

# OBJETIVOS

# OBJETIVO GENERAL

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

# 2.2 OBJETIVOS ESPECÍFICOS

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

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

# ALCANCE

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

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de la CÁMARA DE REPRESENTANTES, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

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

1. Dar cumplimiento a la Ley 1712 de 2014 Ley de Transparencia y el Acceso a la Información Pública.
2. Transparentar los procesos misionales y administrativos de la Entidad.
3. Garantizar la transparencia, la protección y el acceso a la información.
4. Minimizar el riesgo de los procesos misionales de la Entidad.
5. Cumplir con los principios de seguridad de la información.
6. Cumplir con los principios de la función administrativa.
7. Mantener la confianza de los grupos de interés.
8. Apoyar la innovación tecnológica.
9. Implementar el sistema de gestión de seguridad de la información.
10. Proteger los activos de información.
11. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
12. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la CÁMARA DE REPRESENTANTES.
13. Garantizar la continuidad de la gestión frente a incidentes.

Las políticas y lineamientos aquí definidos tienen cobertura sobre los edificios en donde funciona la HCR (Edificio Nuevo, Capitolio, Edificio BBVA y Santa Clara).

# POLÍTICAS GENERALES DE SEGURIDAD TECNOLÓGICA DE LA CÁMARA DE REPRESENTANTES

**OBJETIVO**

Definir los lineamientos generales de seguridad tecnológica de la Cámara de Representantes, con el fin de preservar la disponibilidad e integridad de la información y de todos los elementos que forman parte de a red informática de la Cámara de Representantes.

**ALCANCE**

Esta política debe ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo hardware y/o software de propiedad o en uso por parte de la Cámara de Representantes. Esta política tiene como propósito reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad de las funciones misionales de la Entidad.

**LINEAMIENTOS**

* 1. Usar los computadores en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implementado las medidas de control apropiadas para proteger el software, el hardware y los datos. Estas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
  2. Usar los equipos de cómputo para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
  3. Respetar y no modificar la configuración de hardware y software establecida por la Oficina de Planeación y Sistemas atendiendo a las políticas establecidas en el presente Manual.
  4. No manipular alimentos sobre los equipos computacionales teniendo especial cuidado de no derramar liquido en ellos.
  5. Proteger los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
  6. Toda falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o interrupción de los servicios.
  7. Proteger los equipos para disminuir el riesgo de robo, destrucción, y mal uso.
  8. No mover los equipos o reubicarlos sin autorización previa; para llevar un equipo fuera de la institución se requiere una autorización escrita del Jefe de Planeación y Sistemas; en el caso de los computadores portátiles bastará con la autorización del respectivo jefe inmediato de cada División o Sección.
  9. Reportar inmediatamente a la Dirección Administrativa, pérdida o robo de cualquier componente de hardware o programa de software.
  10. Para prevenir el acceso no autorizado, los equipos están configurados de manera tal que al cabo de diez (10) minutos de inactividad, se active el protector de pantalla y se bloquee el acceso al computador, por lo que se requiere ingresar nuevamente la contraseña para reanudar la actividad. El usuario debe bloquear su computador presionando las teclas CTrl + Alt + Supr ó Windows + L, cada vez que se ausente de su oficina.
  11. El protector de pantalla y fondo de escritorio deben ser los institucionales. No se permite el uso de estos de manera personalizada tanto en los computadores de escritorio como en los portátiles que son propiedad de la Honorable Cámara de Representantes.
  12. Los datos confidenciales que se muestran en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y del protector de pantalla.
  13. En todas las aplicaciones desarrolladas, debe implementarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
  14. No está permitido el uso de módems en los computadores propiedad de la Honorable Cámara de Representantes.
  15. Todo el software de la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido instalar software ilegal (Sin licencia), hacer copias o usar ese software tanto adquirido como desarrollado, para fines personales.
  16. Los usuarios no deben copiar a un medio removible (como DVD, USB, CD, etc.), el software o los datos residentes en las computadoras de la Honorable Cama de Representantes con el propósito de proporcionar información a personal ajeno a la Institución.
  17. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe desconectar de la red y notificar inmediatamente a la Oficina de Planeación y Sistemas, para que se tomen las acciones respectivas.
  18. Debe utilizarse un programa antivirus para examinar todo archivo que venga de afuera o inclusive de manera interna. Este antivirus está instalado de forma predeterminada en cada uno de los computadores de la Cámara de Representantes y administrado por la Oficina de Planeación y Sistemas.
  19. Queda prohibido bajar de Internet, software libre, gratis, demos, y en general software que provenga de una fuente distinta de Entidades Públicas Oficiales. La Dirección Administrativa o la Oficina de Planeación y Sistemas es la responsable de proveer el software de trabajo asignado a cada computador de acuerdo a la disponibilidad de licencias.
  20. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.
  21. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
  22. Cada usuario es responsable de la información almacenada en su computador, por lo tanto, periódicamente debe hacer el respaldo de los datos guardados en PC´s y las copias deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones.
  23. La información de la Cámara de Representantes es clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado y que hayan sido probadas y aprobadas por la Dirección Administrativa y la Oficina de Planeación y Sistemas.
  24. El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y/o personal temporal.
  25. Siempre que sea posible, deberá respaldarse y/o eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar.
  26. El personal que está autorizado y utiliza un computador portátil que contenga información confidencial de la Institución, no debe dejarla desatendida, sobre todo cuando esté de viaje, además esa información debe estar cifrada.
  27. El espacio disponible en los discos duros es para almacenamiento de información relacionada con el trabajo.

# POLÍTICA DE USO DE SERVICIO DE ACCESO A INTERNET

**OBJETIVO**

Definir las pautas generales para asegurar una adecuada protección de la información la Cámara de Representantes cuando se hace uso del servicio de Internet por parte de los usuarios autorizados, definiendo de manera general, no limitativa, las actuaciones consideradas como abusivas y prohibidas.

**ALCANCE**

Esta política se aplica a toda la entidad y a todos los usuarios autorizados para acceder al servicio de Internet incluidos, funcionarios, contratistas y terceros.

**LINEAMIENTOS**

1. El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Cámara de Representantes, los usos diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio.
2. 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.
3. 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.
4. 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.
5. Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red la Cámara de Representantes o descargue desde Internet empleando la cuenta de acceso a Internet que se le ha suministrado.
6. Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ésta u otra Institución.
7. La Cámara de Representantes puede supervisar el acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales, en los procesos verificación del uso apropiado del servicio de acceso a Internet se respetan los derechos a la intimidad y privacidad del titular de la cuenta de acceso a Internet.
8. De manera consistente con prácticas generalmente aceptadas, el Data Center procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la red en el uso de Internet contienen detalles sobre lugares de acceso, número de veces, duración, y fecha y hora en que se efectuó el acceso.
9. Es política de la Oficina de Planeación y Sistemas no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria.
10. 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.
11. Los siguientes usos del servicio de acceso a Internet se consideran usos no autorizados y pueden constituir un incidente de seguridad de la información que se gestionan de acuerdo con los procedimientos adoptados por la Cámara de Representantes:

• El envío o descarga de información sometida a derechos de autor cuando no se tienen esos derechos (música, videos, obras literarias, pictóricas, imágenes)

• El envío, descarga o visualización de información con contenidos que no forman parte de las actividades propias asignadas al usuario

• El uso del servicio de acceso a Internet para actividades comerciales personales.

• El acceso a sitios de música, juegos, vídeos, u otros sitios de entretenimientos on-line.

• El acceso a sitios Web considerados como ilegales por la normatividad colombiana, la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.

• Acceder a lugares obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros.

1. 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.
2. La Oficina de Planeación y Sistemas tiene el deber de filtrar todo contenido que vaya en contra del interés de la Honorable Cámara de Representantes.
3. 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.
4. El uso de Internet es personal e intransferible no permitiéndose que terceras personas hagan uso del servicio.
5. Cada usuario es el responsable de las acciones efectuadas a través de este servicio.
6. La Información consultada en cualquier horario de trabajo a través de Internet, debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del usuario y/o servir como herramienta para desempeñar sus funciones.
7. El usuario no debe utilizar ninguna conexión privada a Internet a través de las estaciones de trabajo conectadas simultáneamente a redes de la Honorable Cámara de Representantes (conexiones celulares).
8. Se prohíbe acceder a redes sociales en las horas laborales.
9. Está prohibido bajar (download), instalar, copiar o almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor.
10. Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que tal información esté cifrada.

**RESPONSABILIDADES**

• Los funcionarios responsables de los procesos de la Entidad son los autorizados para solicitar la creación, modificación o cancelación de las cuentas de acceso al servicio de Internet.

•Todos los funcionarios y contratistas que, en el desarrollo de sus tareas habituales u ocasionales, utilicen el servicio de acceso a Internet de la Entidad son responsables del cumplimiento y seguimiento de las políticas de seguridad de la información la Cámara de Representantes.

• Los responsables de la administración de las redes de acceso a Internet la Cámara de Representantes, deben implementar los controles necesarios para evitar la circulación de información o contenidos desde Internet hacia la red de la Entidad que puedan constituirse en riesgos para la seguridad de la Información.

• Los responsables de la administración de las redes de acceso a Internet la Cámara de Representantes deben implementar los controles de seguridad de la información que reduzcan los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información de la Entidad.

# POLÍTICA DE USO DE SERVICIOS DE CORREO ELECTRÓNICO

**OBJETIVO**

Definir las pautas generales para asegurar una adecuada protección de la información la Cámara de Representantes cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados, definiendo de manera general, no limitativa, las actuaciones consideradas como abusivas y prohibidas.

**ALCANCE**

Esta política aplica a todas los funcionarios, contratistas y terceros que presten sus servicios a la Cámara de Representantes y que por el desarrollo de sus actividades utilizan el servicio de correo electrónico de la Entidad.

**LINEAMIENTOS**

1. El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por la Cámara de Representantes. El uso del servicio de correo electrónico para actividades diferentes a las necesarias para el cumplimiento de las funciones encargadas al funcionario, contratista o tercero requieren autorización del responsable del proceso en el que trabaja la persona.
2. El uso del servicio de correo electrónico la Cámara de Representantes para fines personales no está autorizado.
3. 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.
4. Para crear, activar y desactivar una cuenta de correo electrónico se sigue el procedimiento de gestión de cuentas de usuarios la Cámara de Representantes.
5. El servicio de correo electrónico oficial la Cámara de Representantes es el aprobado por la Oficina de Planeación y Sistemas. Los funcionarios, contratistas y terceros reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.
6. 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.
7. 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 solicitar a la Oficina de Planeación y Sistemas el apoyo para cifrar dicha información.
8. Los correos electrónicos deben contener una nota de confidencialidad ubicada al final del texto, después de la firma del mismo, este mecanismo es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico. La nota de confidencialidad debe seguir el estándar definido por la Cámara de Representantes.
9. 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.
10. Los siguientes usos del servicio de correo electrónico se consideran usos no autorizados y pueden constituir un incidente de seguridad de la información que se gestionan de acuerdo con los procedimientos adoptados por la Cámara de Representantes:

• 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.

1. La Oficina de Planeación y Sistemas en caso de uso no permitido del correo electrónico, suministrará la información del usuario a la entidad que lo requiera para algún tipo de investigación por uso no apropiado del servicio.
2. La cuenta de correo es personal e intransferible no permitiéndose que otros empleados hagan uso de ella.
3. Es responsabilidad del usuario realizar administración de su cuenta periódicamente para que exista espacio disponible.
4. Todo usuario es responsable por los datos/documentos adjuntos que envía.
5. El incumplimiento por parte del usuario de las políticas de uso de servicios de correo electrónico puede ocasionar la suspensión y posterior baja del sistema del servicio de correo electrónico.
6. Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Institución, se debe ejercer cierta cautela al reenviar los mensajes. En todo caso no debe remitirse información confidencial de la Cámara de Representantes sin la debida aprobación.
7. Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco. Y es responsabilidad de cada usuario salvaguardar la información propia de sus labores.

**RESPONSABILIDADES**

• Todos los usuarios del servicio de correo electrónico deben cumplir las políticas de seguridad de la información la Cámara de Representantes.

• Oficina de Planeación y Sistemas es la responsable de la gestión del servicio de correo institucional.

• Los responsables de áreas o procesos deben tramitar la solicitud de asignación de cuenta de correo electrónico para sus funcionarios o contratistas ante la Oficina de Planeación y Sistemas.

# POLÍTICA DE RESPALDO DE INFORMACIÓN

**OBJETIVO**

Definir los lineamientos generales para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información la Cámara de Representantes, y de reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad de las funciones misionales de la Entidad.

**ALCANCE**

Esta política debe ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo realizar, administrar y custodiar las copias de respaldo de la información la Cámara de Representantes.

**LINEAMIENTOS**

1. La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos la Cámara de Representantes, debe ser respaldada conforme a los lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información. Los tiempos de preservación de las copias de respaldo son definidos teniendo en cuenta los requerimientos anteriormente expuestos, así como también la tecnología requerida para la restauración de la información contenida.
2. Para la realización de las copias de respaldo, la Oficina de Planeación y Sistemas junto con el responsable de la información define la información que se debe respaldar, la periodicidad con que se deben realizar las copias y la necesidad o no de mantener copia adicional de los datos respaldados fuera de las instalaciones la Cámara de Representantes.
3. Las copias de respaldo son almacenadas de forma segura por parte de la Oficina de Planeación y Sistemas, para garantizar que no sean manipuladas por personas no autorizadas. Mantiene un registro de todas las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de las mismas: fechas de copia, restauraciones, ubicación de medios.
4. La Oficina de Planeación y Sistemas realiza a intervalos regulares pruebas de restauración de los datos para comprobar su correcto funcionamiento.
5. Las copias de respaldo son almacenadas en lugares que tienen los debidos controles de seguridad, físicos y tecnológicos, que limitan el acceso sólo a las personas autorizadas y garantizan la disponibilidad de la información.
6. Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo, los medios son inutilizados de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas.

**RESPONSABILIDADES**

• La Oficina de Planeación y Sistemas, deben generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.

• Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, de forma controlada y conforme a las necesidades la Cámara de Representantes. Así mismo deberán realizar una prueba periódica de las copias con el fin de validar el correcto funcionamiento y la efectiva restauración.

• Los responsables de la información serán los encargados de verificar administrativamente que las copias de respaldo se realicen de acuerdo con lo establecido y que las estrategias de protección de las copias de respaldo se ajusten a las necesidades y requerimientos la Cámara de Representantes y los responsables de los procesos.

• Los funcionarios, contratistas y terceros la Cámara de Representantes deben almacenar la información requerida para sus procesos operativos, en la ubicación establecida por la Oficina de Planeación y Sistemas dentro del servidor de almacenamiento, con el fin de garantizar la disponibilidad y posibilidad de realización de copias de respaldo de cada una de las áreas de trabajo compartidas de almacenamiento.

# POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN

**OBJETIVO**

Definir las pautas generales para la protección de la información durante el intercambio de la información entre los funcionarios, contratistas y terceros la Cámara de Representantes, y de la entidad con partes externas, preservando las características de disponibilidad, integridad y confidencialidad.

**ALCANCE**

La presente política debe ser adoptada por todos los funcionarios, contratistas y terceros la Cámara de Representantes que en cumplimiento de sus funciones realicen intercambio de información.

**LINEAMIENTOS**

1. La transmisión de la información perteneciente a la Cámara de Representantes se controla según los niveles de clasificación legal de la información establecidos y las políticas de seguridad de la Información la Cámara de Representantes. En caso que se requiera intercambiar información reservada o pública clasificada o sensible personal, se deben adoptar controles de cifrado de información de acuerdo con lo establecido en la política de uso de controles criptográficos la Cámara de Representantes.
2. Los intercambios de información con otras entidades o partes interesadas externas deberán ser soportados por medio de contratos o acuerdos formalizados, determinando en ellos los medios y controles en el tratamiento de la información. Así mismo, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.
3. El uso de la información transmitida o intercambiada deberá realizarse conforme a las características del contrato o acuerdo suscrito con el tercero.
4. La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de *Habeas Data* (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014).

**RESPONSABILIDADES**

• Todos los funcionarios, contratistas y terceros que tengan acceso a la información la Cámara de Representantes, deben protegerla de divulgación no autorizada conforme a los Procedimientos de Clasificación y Etiquetado de la Información definidos en el Sistema de Gestión de Seguridad de la Información **SGSI** la Cámara de Representantes. Se deben usar los mecanismos y controles de seguridad establecidos para el tratamiento de la información. La información sólo podrá ser usada para las actividades autorizadas dentro de los acuerdos suscritos o convenios entre la Cámara de Representantes y las partes interesadas.

• El intercambio de información se efectuará según los acuerdos establecidos, que deben describir: Las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad, los niveles de clasificación de la información a ser intercambiada.

• Para la transferencia de información se deben mitigar los riesgos asociados la pérdida de confidencialidad, integridad o disponibilidad. Se deben emplear canales de transmisión de datos (físicos o lógicos) que permitan brindar los niveles de seguridad apropiados al tipo de información a transmitir. Los canales de transmisión de datos deben preservar los niveles de confidencialidad e integridad de la información, conforme a su nivel de clasificación legal.

• Se deben firmar acuerdos de confidencialidad con las partes interesadas que accedan e intercambien información perteneciente a la Cámara de Representantes, en donde reposen las responsabilidades y se garantice la reserva de la información y el alcance frente al tratamiento de la misma de acuerdo con el marco legal que se aplique a la información a transmitir.

# POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

**OBJETIVO**

Definir los lineamientos generales para controlar el acceso a la información, los activos y sistemas informáticos la Cámara de Representantes.

**ALCANCE**

La política aplica a todos los funcionarios, contratistas y terceros que tengan acceso a la información, activos y sistemas informáticos la Cámara de Representantes.

**LINEAMIENTOS**

1. El Sistema de Gestión de Seguridad de la Información la Cámara de Representantes, busca reducir los riesgos que afectan la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad que se encuentran a cargo de sus funcionarios, contratistas o terceros. Para lograr este objetivo, se han establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente, aquellas clasificadas como áreas seguras, como los centros de procesamiento de información, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado y otras áreas esenciales para el cumplimiento de las funciones misionales de la entidad.
2. El acceso a la información, los sistemas de información y demás recursos de información de la Entidad requiere de una autorización por parte del funcionario responsable de su protección y salvaguarda. La Cámara de Representantes debe contar con procedimientos para tramitar el acceso a la información y sus sistemas de información.
3. Una vez se aprueba el acceso a la información, los funcionarios y contratistas no deben realizar modificaciones sobre la información sin la debida autorización, guardar confidencialidad de la información a la cual tiene acceso, no vulnerar los controles de seguridad establecidos por la Cámara de Representantes, y deben informar al Líder de Seguridad de la Información sobre las debilidades o eventos de seguridad que detecten o sospechen.
4. La Cámara de Representantes lleva a cabo un control de acceso a la información que tiene en cuenta los aspectos lógicos y físicos que permiten garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados.

**RESPONSABILIDADES**

• La información de naturaleza pública la Cámara de Representantes debe de estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.

• El acceso a la información y sistemas de información son controlados conforme a los roles y responsabilidades de los funcionarios y contratistas la Cámara de Representantes. La autorización será otorgada por los responsables de los activos de información. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza la Cámara de Representantes, y así mismo para minimizar el riesgo de la pérdida de integridad o confidencialidad de la información.

• Como responsables de la información, los funcionarios, contratistas y terceros la Cámara de Representantes deberán administrar y hacer cumplir las políticas y controles de seguridad establecidas, con el fin de evitar accesos no autorizados, pérdidas o utilización indebida de los activos de información.

• Los funcionarios, contratistas y terceros la Cámara de Representantes tienen como responsabilidad velar por la integridad, confidencialidad y disponibilidad de la información, los activos y los sistemas informáticos para los cuales han sido designados y autorizados, asegurándose que estos solo sean utilizados para el desarrollo de las labores encomendadas dentro la Cámara de Representantes.

• Los accesos tanto físicos como lógicos, asignados a los funcionarios, contratistas y terceros deben ser desactivados o modificados una vez terminados los vínculos contractuales con la Cámara de Representantes.

• Todos los usuarios tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar su buen uso.

• La Cámara de Representantes establece controles para restringir accesos a áreas seguras, entre otros, deberá registrar los sistemas, datos de identificación de la persona que accede a la información, el motivo de ingreso, el tiempo empleado para el desarrollo de la actividad y, asimismo, cuidará que un responsable del activo de información acompañe a la persona durante su instancia en las áreas definidas como seguras.

• El Responsable o Encargado del activo de información es el responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios autorizados para el acceso a los sistemas de información a intervalos regulares de acuerdo con el nivel de riesgo identificado para el activo de información.

# POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES

**OBJETIVO**

Proteger la confidencialidad, autenticidad o integridad de la información de la Cámara de Representantes a través de medios criptográficos.

**ALCANCE**

La presente política será aplicada para garantizar la confidencialidad, integridad y autenticidad en el tratamiento de la información de la Cámara de Representantes, de acuerdo con los niveles de clasificación determinados y los sistemas electrónicos o de almacenamiento utilizados.

**LINEAMIENTOS**

1. La oficina de Planeación y Sistemas, es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Cámara de Representantes. Con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información la Cámara de Representantes adopta los controles de cifrado de datos que reduzcan los riesgos de seguridad de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la Cámara de Representantes.
2. Para establecer el sistema de cifrado, se tienen en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente.
3. La Oficina de Planeación y Sistemas de la Cámara de Representantes, es la encargada de realizar la respectiva creación, activación, distribución y revocación de las claves criptográficas a los usuarios autorizados y velarán porque la llave se encuentre activa en el período de tiempo previsto.

**RESPONSABILIDADES**

• La solicitud de acceso o actualización al sistema o claves de cifrado se debe efectuar de manera formal a la Oficina de Planeación y Sistemas. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las claves criptográficas, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.

• Los responsables del sistema de cifrado y de las claves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las claves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.

# POLÍTICAS DE SEGURIDAD PARA CONTRASEÑAS Y EL CONTROL DE ACCESO

**OBJETIVO**

Definir los lineamientos generales para la generación, administración y control de acceso de los usuarios, con el fin de preservar la disponibilidad e integridad de la información la Cámara de Representantes.

**ALCANCE**

Esta política debe ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo generar, administrar y controlar las contraseñas y el acceso a servicios de red de la Cámara de Representantes. Esta política tiene como propósito reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad de las funciones misionales de la Entidad.

**LINEAMIENTOS**

* 1. La oficina de Planeación y Sistemas debe asignar los accesos a plataformas, usuarios y segmentos de red, de acuerdo a procesos formales de autorización, los cuales deben ser revisados de manera periódica, con el fin de evitar el acceso de usuarios no autorizados a los sistemas de información.
  2. El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.
  3. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
  4. Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
  5. Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
  6. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
  7. Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
  8. Las contraseñas deben cambiarse con frecuencia, siendo éstas de uso personal, será de responsabilidad de cada usuario acordarse de la contraseña.
  9. Toda contraseña debe empezar con una letra, seguida de un conjunto de caracteres (letra, número o símbolo). Sé recomienda no usar contraseñas que sean fácilmente deducibles.
  10. Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto, la sesión debe ser inmediatamente desconectada.
  11. Para el acceso remoto a los recursos informáticos de la entidad la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas.
  12. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de cinco (5) minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña.
  13. Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
  14. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Honorable Cámara de Representantes pudiendo ser causal de despido.
  15. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
  16. Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.
  17. Los servidores de red deben estar ubicados en sitios apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos sitios y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas lectoras de proximidad).

# 11.1 IDENTIFICACIÓN DE EQUIPOS EN LA RED

• La oficina de Planeación y Sistemas de la Cámara de Representantes debe establecer la dirección MAC como un medio para autenticar las conexiones de ubicaciones y equipos específicos, igualmente debe emplear un mecanismo de control para identificar los equipos que están autorizados a conectarse a la red.

# SEGREGACIÓN EN REDES

• Los dominios de segmentación de la red de la Cámara de Representantes deben ser definidos con base a una evaluación del riesgo y los requerimientos de seguridad diferentes dentro de cada uno de ellos.

• La Oficina de Planeación y Sistemas la Cámara de Representantes establecerá procedimientos de segmentación de la red, tales como:

* Para controlar la seguridad de la red, los grupos de servicios de información, usuarios y sistemas de información, la red la Cámara de Representantes podrá segmentarse en dominios de red lógicos separados a través de VLANs (Redes virtuales LAN).
* Los dominios de segmentación de la red la Cámara de Representantes también se pueden implementar controlando los flujos de datos de la red utilizando capacidades routing/switching, como listas de control de acceso.
* Se debe considerar la segregación de las redes inalámbricas de las redes internas y privadas.

# CONTROL DE CONEXIONES A LA RED

• En la Cámara de Representantes los derechos de acceso a la red de los usuarios se deben mantener y actualizar conforme lo requiera la política de control de acceso.

• Se controlará la capacidad de conexión de los usuarios a través de gateways de la red (pasarelas) a servicios como:

* Mensajería electrónica
* Transferencia de archivos
* Accesos interactivos
* Acceso a una aplicación.

• La política de control de acceso de la Cámara de Representantes puede requerir la incorporación de los controles para restringir la capacidad de conexión de los usuarios en las redes compartidas, en particular cuando estas se extienden a través de los límites o fronteras de la Entidad.

# CONTROLES DE ROUTING DE LA RED

• Los Administradores de Red de la Cámara de Representantes asignados por la oficina de Planeación y Sistemas, deben implementar controles de routing en las redes para asegurar que las conexiones de las computadoras y los flujos de información no afecten la política de control de acceso de los Sistemas de Información.

• Se debe establecer una Zona Desmilitarizada (DMZ) con cortafuegos con el propósito de proteger los servidores de la Entidad.

• Si en las redes de la Cámara de Representantes se emplean tecnologías “proxy” se deben utilizar los gateways de seguridad para validar las direcciones de la fuente y el destino en los puntos de control de las redes internas y externas.

• Las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la Entidad, deben establecer controles de routing.

# IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

• La Oficina de Planeación y Sistemas de la Cámara de Representantes debe establecer un procedimiento para que todos los usuarios de la Entidad cuenten con un identificador único (ID de usuario) para su uso personal, para lo cual:

* Se debe escoger una técnica de autenticación adecuada para validar la identidad de un usuario de la Entidad.
* La identificación automática del usuario se debe considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.
* Se debe aplicar este procedimiento a todos los tipos de usuarios (incluyendo el personal de Soporte Informático, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos).
* Se deben utilizar los IDs de usuarios para rastrear las actividades hasta la última persona responsable.
* No deben realizarse desde cuentas privilegiadas, las actividades de usuarios finales.
* Se requerirá autorización para utilizar un ID de usuario compartido para un grupo de usuarios o un trabajo específico.
* Para autenticación y verificación de identidades sólidas, se deben utilizar métodos de autenticación alternativos para las claves secretas, por ej: medios criptográficos, tarjetas inteligentes, dispositivos o medios biométricos.

# CIERRE DE UNA SESIÓN DE RED POR INACTIVIDAD

• Las aplicaciones y las sesiones de red se cierran después de un período de inactividad definido.

• La Oficina de Planeación y Sistemas debe definir el tiempo mínimo de inactividad de las sesiones de red antes de su cierre.

# POLÍTICAS DE ADMINISTRACION DE HARDWARE Y SOFTWARE

**OBJETIVO**

Definir los lineamientos generales para la administración de hardware y software, con el fin de preservar la disponibilidad e integridad de la información la Cámara de Representantes.

**ALCANCE**

Esta política debe ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo hardware y/o software de propiedad o en uso por parte de la Cámara de Representantes. Esta política tiene como propósito reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad de las funciones misionales de la Entidad.

**LINEAMIENTOS**

1. 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.
2. 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.
3. No deben abrir o romper los sellos de seguridad instalados en cada computador por la Dirección Administrativa y Oficina de Planeación y Sistemas.
4. No abrir, retirar o cambiar componentes de los equipos.
5. Evitar prestar e intercambiar los equipos computacionales.
6. Evitar instalar dispositivos o periféricos sin la supervisión y autorización expresa de la Oficina de Planeación y Sistemas.
7. No retirar o sacar equipo de la institución sin previa autorización del área de almacén.
8. 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 Informática de toda la Cámara de Representantes.
* Estandarizar la seguridad informática, 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.

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Se debe respetar la propiedad intelectual y licencias. El usuario no podrá copiar o redistribuir programas propiedad de la Honorable Cámara de Representantes.
7. 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.

**RESPONSABILIDADES**

La solicitud de acceso o uso de cualquier hardware o software se debe efectuar de manera formal a la Oficina de Planeación y Sistemas. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad de dicho hardware o software.

# POLÍTICAS DE SEGURIDAD PARA REDES

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

1. Todos los cambios en los servidores y equipos de red de la Cámara de Representantes, incluyendo la instalación de un nuevo software y otros, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.
2. Los privilegios especiales, de posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
3. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. La Oficina de planeación y Sistemas debe revocar rápidamente los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
4. Cuando un empleado se retira de la Honorable Cámara de Representantes, la División de Personal debe informar de inmediato a la Oficina de Planeación y Sistemas para que se desactive la cuenta de usuario.

# POLÍTICA DE TELETRABAJO

**OBJETIVO**

Definir las pautas generales para asegurar la información la Cámara de Representantes frente a riesgos asociados al Teletrabajo cuando la entidad haya autorizado y adoptado la estrategia de Teletrabajo definida en la Ley 1221 de 2008.

**ALCANCE**

La política aquí descrita aplica a todos los funcionarios, contratistas y terceros de la Cámara de Representantes que se encuentren autorizados para realizar actividades de Teletrabajo.

**LINEAMIENTOS**

1. La Cámara de Representantes autoriza actividades de Teletrabajo conforme la legislación vigente, las condiciones del trabajo a realizar, los roles y perfiles de los funcionarios, contratistas y terceros de la entidad, y las condiciones previstas por el ordenamiento jurídico colombiano. Las actividades de Teletrabajo sólo se pueden llevar a cabo siempre y cuando se establezcan controles de seguridad alineados con las políticas de seguridad y privacidad de la información de la Cámara de Representantes y frente al respectivo análisis del riesgo.
2. La Cámara de Representantes dispone de los recursos tecnológicos y organizacionales para la adopción de un modelo de Teletrabajo, que permita cumplir con los intereses y necesidades de la entidad, considerando los riesgos y requisitos legales en materia de Teletrabajo.
3. La Cámara de Representantes provee los mecanismos de seguridad física y lógica a los equipos y documentos requeridos para el desarrollo de las actividades de Teletrabajo, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.
4. Para el desarrollo de las actividades de Teletrabajo se debe realizar un análisis de riesgos, a partir del cual se adoptan los mecanismos de control para la protección de la información y los sistemas de información de la Cámara de Representantes accedidos durante las actividades de Teletrabajo.
5. Antes de llevar a cabo cualquier actividad de Teletrabajo, se definen entre La Cámara de Representantes y el funcionario, contratista o tercero el alcance de las actividades a desarrollar y se determinarán como mínimo: la información a acceder, el horario de las actividades y los sistemas y servicios requeridos conforme la necesidad de la Cámara de Representantes y la legislación colombiana vigente.
6. En caso de pérdida o hurto de un equipo en el cual se lleven actividades de Teletrabajo, será responsabilidad del funcionario, contratista o tercero informar de forma inmediata a través de la oficina de Planeación y Sistemas del evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida, seguir los procedimientos legales, administrativos y los procedimientos de atención de incidentes de seguridad de la información.

**RESPONSABILIDADES**

La Oficina Jurídica con el apoyo de la División de Bienes y Servicios, la Oficina de Talento Humano y la Oficina de Planeación y Sistemas, determinará las condiciones de los contratos o acuerdos con los funcionarios, contratistas y terceros, determinando las condiciones, responsabilidades conforme las necesidades de la Cámara de Representantes y la normatividad colombiana vigente para autorizar las actividades de Teletrabajo.

La Oficina de Planeación y Sistemas deberá autorizar el acceso a la información o sistemas de información que puedan ser accedidos a través de los equipos usados para las actividades de Teletrabajo.

La Oficina de Planeación y Sistemas es la responsable de implementar los controles de seguridad de la información necesarios para llevar a cabo las actividades de Teletrabajo.

Los funcionarios, contratistas y terceros que se encuentren autorizados para el desarrollo de actividades de Teletrabajo, deberán cumplir con las responsabilidades y condiciones acordadas, así mismo reportar cualquier situación que pueda afectar el desarrollo de las actividades o ponga en peligro la información de la Cámara de Representantes.

La Oficina de Planeación y Sistemas realizaran campañas de sensibilización para las buenas prácticas de las actividades de Teletrabajo.

La Oficina de Planeación y Sistemas es la responsable de determinar los canales de comunicación y métodos de autenticación apropiados para controlar el acceso de usuarios remotos a la información y sistemas de información de la Cámara de Representantes.

La Oficina de Planeación y Sistemas es la responsable de establecer protocolos que den respuesta a situaciones de alerta como una avería del ordenador causada por un virus, una configuración incorrecta o un fallo de hardware de los equipos autorizados para labores de Teletrabajo.

# POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

**OBJETIVO**

Mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la Entidad, garantizando su continuidad, cumpliendo los niveles de servicio requeridos por los procesos de la Cámara de Representantes y reduciendo los riesgos legales y técnicos a niveles aceptables.

**ALCANCE**

Esta política se aplica a los servicios de computación en nube que sean utilizados o contratados por la Entidad, así como a los procesos que hagan uso de dichos servicios.

**LINEAMIENTOS**

1. En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información institucional, acceso a información personal, protección de secretos comerciales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal.
2. El análisis y gestión de los riesgos se debe realizar de acuerdo con el procedimiento de gestión de riesgos de la Cámara de Representantes Los resultados del análisis y gestión de riesgos se deben documentar de acuerdo con el procedimiento de gestión de riesgo de la Entidad.
3. No se deben utilizar servicios de computación en la nube cuyo análisis de riesgos indique niveles no tolerables para la protección de información institucional o personal. Los resultados del análisis y gestión de riesgos, deben ser determinantes para aceptar o rechazar la utilización de servicios de computación en la nube de pago o gratuitos.
4. En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad de la información de la Entidad, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.
5. En los casos que se requiera el almacenamiento de información en la nube clasificada como reservada, pública clasificada e información de carácter personal esta debe permanecer cifrada para evitar su divulgación o acceso no autorizados. El cifrado se debe realizar de acuerdo con las políticas de seguridad de la información definidas por el sistema de gestión de seguridad de la información de la Cámara de Representantes.

**RESPONSABILIDADES**

Los responsables de procesos de la Cámara de Representantes son los encargados de coordinar la ejecución de las actividades de análisis y gestión de riesgos para el uso de servicios de computación en la nube.

La Oficina de Planeación y Sistemas es la responsable de asistir a los diferentes procesos de la Entidad en la identificación, gestión y tratamiento de los riesgos asociados al uso de servicios de computación en la nube.

Los responsables de los procesos de la Cámara de Representantes son los únicos encargados de tramitar la solicitud de servicios de computación en la Nube una vez analizados los riesgos de seguridad de la información.

Todos los usuarios de servicios de computación en la nube deben aplicar y cumplir los controles de seguridad de la información que se definan con la OPS para el uso seguro de ese tipo de servicios de tratamiento de información.

# TIPOS DE FALTAS

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

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

1. **LEVES**

* Usar los equipos de la Institución, para actividades no laborales como juegos y pasatiempos.
* Manipular alimentos sobre los equipos de cómputo.
* Utilizar fondos y/o protectores de pantalla que no son los institucionales (personalizados), sean computadores personales y/o portátiles, propiedad de la honorable Cámara de Representantes.
* Exponer los equipos a riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
* No reportar inmediatamente fallas en los computadores o en la red que consecuentemente causen problemas serios como pérdida de la información o indisponibilidad de los servicios.
* Mover (cambiar de lugar, desplazar) los equipos o reubicarlos sin autorización previa.
* No reportar a la Dirección Administrativa o a la Oficina de Planeación y Sistemas la detección de, virus u otro agente potencialmente peligroso.
* La no utilización de un programa antivirus para examinar todo archivo que venga de afuera o inclusive de otras Direcciones o dependencias de la Honorable Cámara de Representantes.
* Utilizar Memorias USB u otros medios de almacenamiento en cualquier computador portadores de virus u otros agentes dañinos sin escanear previamente.
* Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.
* La falta de cuidado, pulcritud y limpieza del equipo de informática asignado.
* La navegación en Internet para fines personales por períodos prolongados de tiempo.
* Bajar archivos de música o vídeo desde Internet.

1. **MENOS GRAVES:**

Constituyen faltas menos graves:

* La reincidencia en la comisión de una falta leve
* Modificar la configuración de hardware y/o software establecida por la Dirección Administrativa o la Oficina de Planeación y Sistemas.
* La instalación de programas y la modificación de los programas, paquetes y configuraciones ya instalados en los computadores.
* Visitar o acceder a sitios web obscenos, que distribuyan material pornográfico, o materiales ofensivos en perjuicio de terceros.
* Utilizar el Internet para enviar mensajes que vayan en contra de empleados y/o de los intereses de otras personas, así como de ésta u otra Institución. Por ejemplo (cadenas correos masivos).

1. **GRAVES:**

Constituyen faltas graves:

* La reincidencia en la comisión de una falta menos grave
* La pérdida o robo de cualquier componente de hardware o programa de software por negligencia o dolo debidamente comprobado.
* Revelar datos confidenciales.
* Hacer copias o usar software tanto adquirido como desarrollado, para fines personales y en violación a derechos de autor.
* Hacer uso de software bajado de Internet (software libre, gratis, demos, etc.) y en general software que provenga de una fuente no confiable.
* El uso de módems en PCs que tengan también conexión a la red local (LAN.
* Copiar a un medio removible (como un DVD, USB, CD), el software o los datos residentes en las computadoras de la Honorable Cámara de Representantes, sin la aprobación previa.
* No realizar respaldos de los datos guardados en PCs y servidores.
* Negligencia en el manejo de la información confidencial de la Honorable Cámara de Representantes contenida en computador personal o portátil.
* Borrar/eliminar la información original no cifrada sin que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
* Utilizar/usurpar el acceso a las claves utilizadas para el cifrado y descifrado.
* Abrir los equipos de cómputo, violentar sellos.
* Prestar, compartir, usurpar la contraseña.
* Burlar los sistemas de seguridad informática.
* Sacar (extraer) o cambiar componentes de los equipos
* Prestar e intercambiar los equipos de cómputo sin la correspondiente autorización.
* Instalar equipos sin la supervisión y autorización expresa de la Oficina de Planeación y Sistemas.
* Leer, copiar, o cambiar los archivos de cualquier otro usuario.
* Inspeccionar, copiar y almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor.
* Enviar a través de Internet mensajes con información confidencial a menos que tal información esté cifrada y autorizada.
* Divulgar, duplicar, modificar, destruir, extraviar, robar y acceder a información confidencial.

# TERMINOS Y DEFINICIONES

**Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

**Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

**Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

**Análisis de riesgos:** proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.

**Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas). Direcciones y demás información de contacto. Números identificativos. Apodos o cargo.

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

**Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.

**Autenticidad:** Propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

**Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

**Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

**Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Clave (Llave) Criptográfica** Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

**Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

**Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

**Datos abiertos:** son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano. Con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

**Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

**Dato personal:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados. Ley 1266/2008

**Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

**Dato privado**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

**Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

**Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

**Disco duro**: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

**Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**Documento en construcción**. Son documentos que no cumplen las condiciones de ser documentos públicos si es información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal. De acuerdo con la Sentencia C-274-13 de 5 de marzo de 2014, un sujeto obligado puede mantener la reserva sobre información preliminar, dependiendo de que esta reserva obedezca a (i) un fin constitucionalmente legítimo (ii) la medida resulte ser razonable, proporcionada y necesaria.

**DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

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

**Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

**Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.

**Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

**Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

**Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

I**nformación**. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen Ley 1712/2014

**Información pública,** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, Ley 1712/2014.

**Información pública clasificada**. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712/2014;

**Información pública reservada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712;

**Impacto:** el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

**Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.

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

**Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012).

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

**Laptop:** Computador Portátil.

**Llave criptográfica.** Ver clave criptográfica.

**No repudio**: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

**Parte interesada (*Stakeholder*):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**Perfil de acceso:** mecanismo de seguridad mediante el cual se definen los permisos de acceso de usuario o grupo de usuarios a un conjunto de información o sistema de información

**Plan de continuidad del negocio**: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

**Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

**Proceso**: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

**Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

**Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

**Responsable del tratamiento:** persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

**Rol:** función que alguien o algo desempeña.

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

**Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

**Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

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

**Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

**Suplantación de Identidad:** Se entiende por *suplantación de identidad* aquella acción por la que una persona se hace pasar por otra para llevar a cabo cualquier actividades.

**Teletrabajo:** actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo.

**Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

**Tercero:** hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.

**Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

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

**Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

# RESPONSABLE DEL DOCUMENTO

Jefe de Planeación y Sistemas Cámara de Representantes

|  |  |  |  |
| --- | --- | --- | --- |
| **REGISTRO DE CAMBIOS AL DOCUMENTO** | | | |
| FECHA | VERSION | DESCRIPCION | ELABORADO POR: |
| 2020/07/02 | 2.0 | Construcción/Actualización de políticas y lineamientos solicitadas por el jefe de la OPS | Jorge Armando Guarín |