POLÍTICA DE CONTROL DE ACCESOS

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

Bogotá – Colombia
Noviembre de 2020

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

El presente documento establece las políticas y normas para garantizar un adecuado control de acceso a los sistemas de información de la Cámara de Representantes.

Para la Entidad es prioritario definir el personal que tiene acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones tecnológicas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. En tal sentido, se hace necesario controlar y restringir el acceso a toda la información sin importar si se encuentra en medios físico y/o digitales, garantizando así, la confidencialidad e integridad de ésta.

2. OBJETIVOS

2.1 GENERAL

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la Cámara de Representantes se encuentren debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

2.2 OBJETIVOS ESPECÍFICOS

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas y de la información.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de claves, equipos de cómputo e información.
- Garantizar la seguridad de la información cuando se utiliza computación móvil y/o trabajo remoto.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

El presente documento tiene aplicabilidad a todas las formas de acceso de todos los colaboradores, contratistas o terceros a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos, documentación, programas o servicios de información, sin importar la función que desempeñe en la Entidad.

4. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
Ley 594	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones
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 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 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 1727	2009	Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información
Ley 734	2002	Por la cual se expide el Código Disciplinario Único

5. DEFINICIONES Y TÉRMINOS

Activo: Cualquier cosa que tenga valor para la organización. (ISO/IEC 13335-1:2004).

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 dicho fin.

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Cámara de Representantes en un momento dado.

Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la Entidad.

Acceso lógico: En general, el acceso lógico es un acceso electrónico o digital, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los

servicios de procesamiento de información sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Incidente: Cualquier evento que no forma parte de una operación normal de un servicio y que causa o puede causar una interrupción o reducción de la calidad del servicio.

6. DESCRIPCIÓN DE LA POLÍTICA

La Cámara de Representantes debe establecer las medidas de control de acceso a toda la información propiedad de la Entidad, sin importar el medio en el que se almacene, procese, utilice, transmita, lo cual incluye, pero no limita a recursos de físicos y digitales; ambientes públicos, privados, propios, de terceros o en nube; redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, entre otros.

Los controles de acceso deben ser idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Entidad. Éstos deben ser conocidos por todos los funcionarios, colaboradores y terceras partes que cuentan con privilegios de acceso a la información de la Entidad y deben controlar los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función.

Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

6.1 LINEAMIENTOS GENERALES DE CONTROL DE ACCESO

La Oficina de Planeación y Sistemas estará a cargo de definir normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información, el monitoreo del uso de las instalaciones de procesamiento de la información, el uso de dispositivos móviles, y reportes de incidentes relacionados; la revisión de registros de actividades; y el ajuste de relojes de acuerdo con un estándar preestablecido. Además, es responsable de:

- Establecer los mecanismos de control de acceso necesarios con base a los requisitos de seguridad de la información y de los requisitos propios de la Entidad.
- Definir, implementar y monitorear los controles de acceso adecuados para proteger la

información y las instalaciones en donde se procesa, almacena, trata y se transmite.

- Analizar y realizar seguimiento permanente de las medidas de control de acceso utilizadas, verificando su eficiencia y efectividad.
- Permitir el acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la Cámara de Representantes únicamente a los usuarios que hayan sido permitidos específicamente y de acuerdo con el propósito de sus funciones y responsabilidades, verificando los privilegios otorgados sobre los activos de información.
- Se debe realizar la asignación del menor privilegio frente a los activos de información de la Entidad. Los mismos deben ser otorgados únicamente por el tiempo que sea necesario para la ejecución de las funciones y actividades propias del rol.
- Realizar el registro de las actividades relacionadas con el acceso a los activos de información de la Entidad, realizando auditorías continuas sobre los mismos y verificando el cumplimiento de los lineamientos y ejecución efectiva de los procedimientos asociados.
- Verificar el cumplimiento de los lineamientos establecidos, relacionados con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos.

6.2 RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- El **Responsable de la Seguridad y Privacidad de la Información** estará a cargo de definir normas y procedimientos para la gestión de accesos a todos los activos de información, así como de las instalaciones en donde se procesa o almacena información confidencial. Los accesos y privilegios deben ser limitados únicamente a personas autorizadas. Además, es responsable de:
    - Definir las directrices y los lineamientos para la conexión a los activos de información de Información, de forma segura y confiable.
    - Verificar la asignación de privilegios a usuarios.
    - Analizar y sugerir medidas a ser implementadas para que el control de acceso a los activos de información y servicios de la Entidad, así como verificar su cumplimiento y su efectividad.
    - Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, verificación de que se ejecuten los procesos de auditoría.
    - Apoyar a los usuarios sobre el uso apropiado de claves y de equipos de trabajo.
    - Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.

- Acceder a los registros de auditoría a fin de realizar el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

6.3 RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Los propietarios de los activos de información deben determinar las normas de control de acceso y la asignación de los privilegios sobre ésta, de acuerdo con la política de seguridad de la información y el análisis de riesgos. Así mismo, son los responsables de:

- Identificar toda la información que corresponda a su área de responsabilidad cualquiera que sea su forma y medio de conservación.
- Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de éstos y mantener un registro actualizado de la información más sensible.
- Autorizar el acceso sobre sus activos de información a colaboradores, contratistas o terceros de la Entidad, de acuerdo con sus respectivas funciones.
- Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales.

6.4 ACCESO A REDES Y A SERVICIOS DE RED

El acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la Cámara de Representantes debe ser otorgado únicamente a los usuarios que hayan sido permitidos específicamente y según a sus funciones y responsabilidades.

6.4.1 UTILIZACIÓN DE LOS SERVICIOS DE RED

Las conexiones no seguras a los servicios de red pueden afectar a la Entidad, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de éstos.

El responsable de la Oficina de Planeación y Sistemas tendrá a cargo otorgar el acceso y los privilegios sobre los servicios y recursos de red, únicamente a través de la solicitud formal del responsable del área correspondiente del personal a su cargo y para cumplimiento de las funciones asignadas. Para ello, se debe desarrollar procedimientos para la activación y desactivación de derechos de acceso a las redes y servicios de información, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a la información y a los servicios de red.

- Establecer controles para la identificación y autenticación de los usuarios otorgados a terceros a las redes o recursos de red de la Entidad.
- Establecer los mecanismos necesarios para realizar conexiones seguras a los servicios de red y a la información, desde cualquier lugar y/u origen, lo cual incluye accesos remotos y teletrabajo para los funcionarios que por su labor así lo requieran. Los accesos deben ser aprobados, registrados y auditados.
- Los funcionarios y terceros que requieran acceder a los activos de información a través de sus equipos personales deben cumplir con todos los requisitos o controles para autenticarse y únicamente podrán realizar las funciones para las que fueron autorizados.
- Todos los funcionarios y terceras partes jurídicas o naturales deben cumplir las Políticas de Seguridad y Privacidad de la Información y firmar todos los acuerdos y cláusulas estipuladas para tener acceso a los sistemas de información de la Entidad.

6.4.2 ACCESO A INTERNET

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. Los accesos serán autorizados formalmente por jefe del área correspondiente y a cargo del personal que lo solicite. Así mismo, se debe dar un uso adecuado y racional por parte de los colaboradores.

6.4.3 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Todos los usuarios tendrán un identificador único (ID de usuario) solamente para su uso personal y exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no deben indicar ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la Entidad, podrá utilizarse un código de usuario compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se debe documentar la justificación y aprobación del propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo, autenticador de hardware), deberá implementarse un procedimiento que incluya:

- Asignar la herramienta de autenticación.
- Registrar los usuarios autorizados.
- Revocar códigos de acceso al momento de la desvinculación de los colaboradores, contratistas o terceros.
- Revocar códigos de acceso, en caso de compromiso de seguridad.

6.5 GESTIÓN DE ACCESOS DE USUARIOS

La Entidad debe implementar controles y procedimientos formales con el objeto de impedir el acceso no autorizado a la información y de garantizar la confidencialidad, disponibilidad e integridad de la información; y establecerá la asignación de derechos de acceso a los sistemas, a las redes de datos, los recursos tecnológicos y los servicios de información.

Así mismo, velará porque los funcionarios, contratistas, terceras partes, y todo aquella persona natural o jurídica que tenga interacción con la información de la Cámara de Representantes, tengan acceso únicamente a la información necesaria para el desarrollo de sus funciones y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

6.5.1 REGISTRO Y CANCELACIÓN DE REGISTRO DE USUARIOS

- La Oficina de Planeación y Sistemas debe registrar todos los usuarios en la Base de Datos de Usuarios especificando y/o asociando el rol a desempeñar.
- La creación de un nuevo usuario solo será realizada después de la solicitud formal de acuerdo con los procedimientos establecidos, y bajo la aprobación explícita del responsable del área, de lo contrario no se efectuará el trámite de dicha solicitud.
- Se deben utilizar métodos para proporcionar una identidad reconocible bajo códigos de identificación únicos, de manera que se puedan relacionar sus acciones y evitando la existencia de múltiples identificadores de acceso para un mismo empleado.
- Se debe verificar que el usuario tiene autorización del Propietario de la Información para el uso de la información, del sistema, base de datos o servicio de información.
- Se debe verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario.
- Se debe mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Se debe cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron su rol o de aquellos a los que se les revocó la autorización, se desvincularon de la Entidad o sufrieron la pérdida/robo de sus credenciales de acceso.

6.5.2 GESTIÓN DE PRIVILEGIOS

- Se debe identificar, limitar y controlar la asignación y el uso de los accesos privilegiados de cada sistema, proceso o servicio.
- Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación.

6.5.3 GESTIÓN DE CLAVES DE USUARIO

La asignación de claves se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento de las credenciales de acceso y/o información de autenticación.
- Garantizar que los usuarios cambien las claves iniciales que les han sido asignadas la primera vez que ingresan al sistema.
- Generar claves temporales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la clave y los usuarios deben dar acuse de recibo cuando la reciban.
- No compartir las credenciales de acceso.
- Almacenar las claves sólo en sistemas informáticos protegidos.
- Configurar un estándar de claves de acceso.
- Cambiar las credenciales de acceso a los sistemas que han sido utilizados por personal externo, luego de realizar sus actividades.

6.5.4 GESTIÓN DE CLAVES CRÍTICAS

En los diferentes ambientes de procesamiento existen códigos de usuarios con los cuales es posible efectuar actividades críticas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software y configuración de componentes informáticos. Dichas cuentas no serán de uso habitual, sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por claves con un mayor nivel de complejidad que el habitual.
Las cuentas con accesos privilegiados deben ser controladas y gestionadas a través de los mecanismos necesarios para garantizar el gobierno y protección sobre éstas.

6.5.5 REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS

El área de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad y Privacidad de la Información establecido en la Cámara de Representantes debe efectuar un proceso formal de revisión, a intervalos regulares, a fin de verificar los derechos de acceso de los usuarios y de mantener un control eficaz del acceso a los datos y servicios de información. Para ello, la Entidad debe contemplar los controles necesarios, entre otros, los siguientes:

- Revisar los derechos de acceso de los usuarios a intervalos planificados y registrar los cambios que se realicen.
- Colocar límites de tiempo para los derechos de acceso con privilegios especiales.

- Revisar las asignaciones de privilegios a intervalos planificados, a fin de garantizar que no se obtengan privilegios no autorizados.
- Revisar los derechos de acceso a la terminación del contrato de los funcionarios o cambios dentro de la Entidad (cambios de funciones o promociones).

6.6 RESPONSABILIDAD DEL USUARIO

Los colaboradores, contratistas y terceros que hacen uso de los activos de información de la Cámara de Representantes son responsables de las acciones que, realizadas sobre los mismos, así como de las credenciales de acceso que le son asignadas para su uso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad de la información, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el uso y ejecución de controles de acceso eficaces, en particular aquellos relacionados con el uso de credenciales y la seguridad de los equipos de cómputo y a la información.

Ningún colaborador debe compartir sus cuentas de usuario, contraseñas y/o factores de autenticación asignados para el ingreso a los servicios de red y sistemas de información con otros colaboradores, funcionarios o terceros.

Los funcionarios, colaboradores, contratistas y terceros que posean acceso a los activos de información de la Cámara de Representantes deben acogerse a las normas y mejores prácticas establecidas para la configuración de contraseñas asignadas por la Entidad.

Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por clave.

Todos los escritorios físicos y digitales deben permanecer despejados con el fin de reducir los riesgos de acceso no autorizado, pérdida o daño de la información durante la jornada laboral o fuera de ella.

6.7 USO DE CONTROLES DE AUTENTICACIÓN

Las claves constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. En tal sentido la Cámara de Representantes debe establecer e implementar las normas para el uso de las credenciales de acceso y los factores de autenticación proporcionados a los usuarios, teniendo en cuenta las mejores prácticas, entre las cuales se establecen las siguientes:

- Los usuarios de los diferentes sistemas de información de la Entidad deben seguir buenas prácticas de seguridad en la selección y uso de claves.
- Los usuarios con accesos a los activos de información deben mantener las claves en secreto, no divulgarlas ni compartirlas.

- Las contraseñas deben ser cambiadas cada vez que el sistema se lo solicite o siempre que exista un posible indicio de compromiso del sistema o de las claves. Así mismo, las claves temporales deben cambiarse en el primer inicio de sesión.
- Evitar registrar y/o almacenar las credenciales de acceso en cualquier tipo de elemento físico y/o digital.
- Las contraseñas utilizadas por los usuarios deben ser robustas con el fin de evitar que sean comprometidas fácilmente. Las mismas no deben estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, datos generales, o de la Entidad. Las mismas, no deben tener caracteres idénticos consecutivos o grupos totalmente numéricos o alfabéticos.
- Evitar incluir claves en los procesos automatizados especialmente en los relacionados con el inicio de sesión
- Notificar cualquier incidente de seguridad relacionado con sus claves: pérdida, robo o indicio de pérdida de confidencialidad.

6.8 CONTROL DE ACCESO AL SISTEMA Y LAS APLICACIONES

6.8.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

La información es un activo de vital importancia para la Entidad. y como tal debe ser protegido y contar con los mecanismos de control de acceso más adecuados. El acceso a la información está dado directamente por medio de los programas o aplicativos que manejan los datos y que son operados directamente por los usuarios autorizados; o indirectamente por medio de programas utilitarios que son operados por personal de soporte. En cualquiera de los casos se deben consideren los diferentes controles de frente al acceso a la información:

- El acceso de los usuarios a los sistemas, a la información, a las aplicaciones, o a los recursos de la Entidad, debe ser limitado de acuerdo con sus responsabilidades y funciones.
- Existirán privilegios de acceso a la información, debidamente definidos por los propietarios de la información y estos privilegios deben usarse de una manera responsable por parte de los usuarios y no se debe realizar o intentar acceder a información para la cual no se está autorizado.
- Se debe controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Se deben considerar mecanismos de control de acceso físicos y lógicos adicionales para sistemas o información sensible.

6.8.2 INGRESO SEGURO A SISTEMAS Y APLICACIONES

La Entidad debe establecer los mecanismos para garantizar el acceso controlado y seguro a los sistemas, aplicaciones y activos de información de la Entidad. Así mismo, se debe propender por:

- El mecanismo de acceso debe de corroborar que corresponde a un usuario específico, por lo cual corrobora la identidad del usuario.
- Considerar autenticación sólida y robusta, a través del uso de otros factores de autenticación adicionales al usuario y contraseña, principalmente para los sistemas e información crítica.
- Evitar que cualquier información relacionada con el activo de información sea entregada al usuario que realiza el procedimiento de ingreso, sin que éste haya sido exitoso, y solo en caso de que sea absolutamente necesario hacerlo.
- Los mecanismos de acceso a los activos de información de la Entidad deben ser sometidos a pruebas periódicas de seguridad, con el propósito de identificar y gestionar los riesgos y vulnerabilidades asociados a dichos componentes.
- Realizar el registro de las actividades sobre los accesos a la información de la Entidad.
- La transmisión de las credenciales de acceso y de los mecanismos de autenticación debe realizarse mediante algoritmos de cifrado robustos y no vulnerables.
- Las sesiones inactivas deben ser finalizadas de forma automática por los sistemas y aplicaciones.

6.8.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS

Las contraseñas constituyen uno de los principales medios de validación y autorización de permisos a un usuario para acceder a un servicio informático. Los sistemas de administración de credenciales deben constituir una herramienta eficaz e interactiva que garantice contraseñas robustas. El sistema de administración de credenciales debe:

- Imponer el uso de mecanismos de acceso individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas
- Imponer el uso de contraseñas robustas y rechazar contraseñas débiles.
- Obligar a los usuarios a cambiar las claves temporales en su primer procedimiento de autenticación.
- Evitar mostrar las claves en pantalla cuando son ingresadas.

6.8.4 USO DE UTILITARIOS DE SISTEMA

Los programas utilitarios que podrían tener la capacidad de pasar por alto las seguridades de los sistemas y aplicaciones, por lo cual su uso debe ser limitado y minuciosamente controlado. Se deben considerar los siguientes aspectos:

- Utilizar procedimientos de autenticación para utilitarios del sistema y programas con funciones administrativas.
- Separar los utilitarios de las aplicaciones del Sistema y segregar las funciones cuando sea

posible.

- Limitar el uso de utilitarios del sistema únicamente a usuarios fiables y autorizados.
- Evitar que personas ajenas a la Entidad tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en los recursos informáticos.

6.8.5 CONTROL DE ACCESO AL CÓDIGO FUENTE

- El código fuente de propiedad de la Entidad debe ser protegido frente al acceso no autorizado.
- Establecer los controles para mantener registros de auditoría de los cambios realizados en el código fuente propietario de la Entidad.
- La Entidad debe tener ambientes de desarrollo apropiados y con todas las características de aseguramiento con el fin de proteger el ciclo de vida del software desde su inicio y en su etapa de operación y mantenimiento.

6.9 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS

Se deben generar registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad de acceso a las aplicaciones, programas e información. Los registros de auditoría deberán incluir como mínimo los siguientes datos:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados.

7 RESPONSABLES

- **Oficial de Seguridad de la Información**: Velar por el cumplimiento de la presente política para garantizar el adecuado control de acceso lógico y físico definido por la Cámara de Representantes.
- **Jefe de la Oficina de Planeación y Sistemas**: Poner a disposición los recursos necesarios para el cumplimiento de los lineamientos descritos en la presente política.
- **Oficina de Personal**: Deberán informar a la Oficina de Planeación y Sistemas cuando finalice el contrato de cualquier miembro del personal de planta de la Cámara de Representantes.
- **Jefe del área Jurídica**: deberá informar a la Oficina de Oficina de Planeación y Sistemas cuando finalice el contrato de funcionarios y contratistas.
- **Todos**: No deberán acceder a las áreas seguras sin autorización, a excepción que sea en

cumplimiento de sus obligaciones con la Cámara de Representantes.

- Dar cumplimiento a esta política.

8 INCUMPLIMIENTO

El incumplimiento de la Política de Gestión 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.*
- International Organization for Standardization, *ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems.*
- Icontec Internacional Guía Técnica Colombiana NTC-ISO/IEC 27002, *Técnicas de seguridad. Código de Práctica para controles de seguridad de la información - 2015.*

10 CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
1	16/12/2021	• 19/10/2020 Creación del Documento. • 06/11/2020 Cambio de Formato. • 25/11/2020 Cambio de Formato.	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.