POLÍTICA DE INTEGRIDAD

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

Bogotá – Colombia
Octubre de 2020

INDICE DE CONTENIDO

1. INTRODUCCIÓN

Este documento establece la Política de Integridad de los Sistemas y la Información de la Cámara de Representantes para garantizar la propiedad de integridad de la información. Por ello, la Entidad ha optado por adoptar los principios de integridad de los activos de información establecidos en la norma NIST SP 800-53 como la directriz oficial para este documento y sigue prácticas definidas en las normas y estándares definidos para el Sistema de Gestión de Seguridad de la Información y del Modelo de Seguridad y Privacidad. Las siguientes subsecciones esbozan los lineamientos de integridad del sistema y la información que constituyen la política de la Cámara de Representantes.

El presente documento establece los lineamientos del manejo y aseguramiento de la integridad de la información, conocida o administrada por usuarios internos y externos relacionados con la Cámara de Representantes.

2. OBJETIVOS

2.1. GENERAL

Definir la política de la Cámara de Representantes para garantizar la integridad de los activos de información.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

Esta política se aplica a todos los colaboradores, terceros y contratistas de la Cámara de Representantes con acceso a:

- Los activos de información de la Cámara de Representantes, independientemente de su ubicación.
- A activos de información de otras Entidades del Estado.
- A activos de información de terceras partes que tengan vínculo con la Cámara de Representantes.

Cada área de la Cámara de Representantes está obligada al cumplimiento de esta política, y debe desarrollar o adherirse al cumplimiento de la política y al seguimiento de los procedimientos y estándares documentados para tal fin.

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

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 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 734	2002	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.

Información: Según el Artículo 6°. Definiciones, de la Ley 1712 de 2014, “Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen”.

Autenticación: Es un proceso que garantiza y confirma la identidad de un usuario. La autenticación es uno de los aspectos básicos en la seguridad de la información, junto con los tres pilares, a saber: la integridad, disponibilidad, y confidencialidad.

Comunicación: Intercambio de información entre dos o más usuarios a través de medios de transmisión alámbrico o inalámbricos por medio de señales eléctricas de tensión o corriente. El elemento que suministra la información se denomina emisor y el (los) que la(s) recibe(n) se denomina(n) receptor(es).

Acceso lógico: En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.

Log: Es un archivo en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

6. DESCRIPCIÓN DE LA POLÍTICA

Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida exclusivamente a las personas y mediante los medios autorizados por la Cámara de Representantes, asegurando en todo momento su integridad y evitando modificaciones y/o

alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información.

6.1. LINEAMIENTOS

- **Referente a la información en general:** Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas autorizadas y a través de los medios correspondientes, sin modificaciones ni alteraciones**.**
- **Transmisión de la Información**: Para la información que se clasifique como Reservada, Clasificada, Pública, y requiera ser transmitida a través de canales de comunicación se deben utilizar mecanismos que permitan garantizar que la información mantiene su integridad mientras es transmitida por la red, es decir, que la información es completa y exacta de punto a punto en la transmisión.
- **Procedimientos de integridad del sistema y de la información**: Todas las áreas de la Cámara de Representantes deben desarrollar, adoptar o adherirse a un sistema formal y documentado que aborde el propósito, el alcance, las funciones, las responsabilidades y el compromiso de gestión frente a los activos de información.
- **Solución de fallas**: En todos los sistemas que almacenen información de la Cámara de Representantes se deben identificar y reportar las fallas del sistema de información e incorporar la corrección de fallas en el proceso de gestión de la configuración.
- **Protección de código malicioso**: Los sistemas que almacenen información de la Cámara de Representantes deben emplear mecanismos de protección de códigos maliciosos en puntos de entrada y salida de información en la red para detectar y erradicar códigos maliciosos.
- **Supervisión del sistema de información**: Para todos los sistemas que almacenen información de la Cámara de Representantes se debe tener en cuenta:
    - Monitorear eventos en el sistema de información y detectar ataques a estos.
    - Identificar el uso no autorizado de los activos de información.
    - Implementar dispositivos de monitoreo estratégicamente dentro del activo de información para recopilar información esencial determinada por la Entidad, y en ubicaciones ad-hoc dentro del sistema para rastrear tipos específicos de transacciones de interés para la Entidad.
    - Aumentar el nivel de actividad de monitoreo de activos de información siempre que haya un indicio de un mayor riesgo para las operaciones y activos de la Entidad, colaboradores, otras Entidades estatales o la Nación en base a información policial, información de inteligencia u otras fuentes de información.
    - Obtener opinión legal con respecto a las actividades de monitoreo de activos de información de acuerdo con las leyes, directivas, políticas o regulaciones aplicables.

- **Alertas de seguridad, avisos y directivas**: Todos los sistemas que almacenen información de la Cámara de Representantes deben generar alertas, avisos y directivas de seguridad interna según se considere necesario.
- **Verificación de la funcionalidad de seguridad**: Para los sistemas que almacenen información de la Cámara de Representantes se debe verificar al menos anualmente la configuración de seguridad y notificar al administrador del sistema cuando se descubren anomalías con el fin de garantizar una acción correctiva oportuna.
- **Integridad del software y la información**: Los sistemas que almacenen información de la Cámara de Representantes deben detectar cambios no autorizados en el software.
- **Restricciones de ingreso de información**: Todos sistemas que almacenen información de la Cámara de Representantes deben restringir la capacidad de ingresar información al activo de información al personal autorizado.
- **Validación de entrada de información**: Todos los sistemas que almacenen información de la Cámara de Representantes deben verificar la validez de las entradas de información para los activos de información de la Entidad.
- **Manejo de errores**: En todos los sistemas que almacenen información de la Cámara de Representantes se debe:
    - Identificar condiciones de error potencialmente relevantes para la seguridad.
    - Estructurar los mensajes de error con el fin que brinden la información necesaria para las acciones correctivas sin revelar información sensible de la Entidad en los registros de errores y mensajes administrativos que podrían ser explotados por los adversarios.
    - Los mensajes de error solo los debe conocer el personal autorizado.
- **Manejo y retención de la salida de información**: Todos los sistemas que almacenen información de la Cámara de Representantes deben manejar y retener tanto la información dentro como la salida del sistema de información de acuerdo con las leyes, directivas, políticas, regulaciones y estándares aplicables.

7. RESPONSABLES

- La Oficina de Planeación y Sistemas debe:
    - Gestionar los datos tanto internos como externos de manera segura.
    - Asegurar que cualquier contrato de la Cámara de Representantes se adhiere a cualquier Ley, procedimientos y normas pertinentes y a las políticas de la Oficina de Planeación y Sistemas.
    - Asegurarse que el personal de la Entidad conoce todas las sanciones aplicables por incumplimiento.
    - Elaborar y aplicar políticas y procedimientos a nivel de los sistemas, para cumplir con cualquier requerimiento adicional, pertinente y estatutario de integridad de la información.
    - Asignar un propietario para cada componente de infraestructura (por ejemplo, red,

firewall) respaldado por la Oficina de Planeación y Sistemas.

- Asegurar que los controles de seguridad y privacidad que minimizan los riesgos frente a los activos de información se encuentren debidamente implementados, actualizados y configurados.
- Utilizar procedimientos operativos estándar para gestionar los cambios necesarios.
- Utilizar herramientas de verificación de integridad para detectar cambios no autorizados en el software y la información.
- Protección del sistema de información frente a la ejecución de código no autorizado.

- Los **Responsables de los Activos de Información** deben:
  - Realizar el análisis de riesgos de seguridad digital de frente a los activos de información bajo su responsabilidad.
  - Velar por la implementación de los controles que aseguran y protegen los activos de información a su cargo.
  - Asegurar que se Implementación de directivas de seguridad y privacidad de la información.
- El **Responsable de la Seguridad de la Información** debe:
  - Realizar exploraciones de seguridad del sistema de información programadas.
  - Verificar la protección de los sistemas de información.
  - Monitoreo de sistemas de información.
  - Velar por la integridad de la información de la Cámara de Representantes.
- Todos los **colaboradores**:
  - Dar cumplimiento a esta política.

8. INCUMPLIMIENTO

El incumplimiento de la Política de Integridad 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.*

- Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 – 2020

10. CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
1	16/12/2021	• 19/10/2020 Creacion del Documento. • 24/11/2020 Ajuste 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.