POLÍTICA DE ESCRITORIO LIMPIO

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

Bogotá – Colombia
Noviembre de 2020

INDICE DE CONTENIDO

1. INTRODUCCIÓN

La Cámara de Representantes entiende el valor de la información para el cumplimiento de su misión y, por ello debe protegerlos para reducir y gestionar los riesgos de acceso no autorizado y pérdida o daño de la información que se encuentra en medios físicos impresos o en medios de almacenamiento digital.

Por tal motivo, la siguiente Política define los lineamientos y medidas preventivas que permiten establecer una postura de seguridad de frente a la información que es creada, utilizada, procesada y almacenada en medios físicos y digitales y que son empleados en los puestos de trabajo de los funcionarios, contratistas, terceros y, en general, cualquier persona que interactúe con la información de la Entidad.

2. OBJETIVO

2.1. OBJETIVO GENERAL

Establecer los lineamientos para que todo el personal, funcionarios, contratistas y terceros que interactúan con la información de la Cámara de Representantes apropien las mejores prácticas de seguridad y privacidad de la información que permitan reducir los riesgos de acceso no autorizado, daño, pérdida o divulgación no autorizada de la información que crean, utilizan, procesan, almacenan, en sus puestos de trabajo, equipos de cómputo, unidades de almacenamiento extraíble, contenedores físicos de información, de toda aquella información física y digital , con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información.

2.2. OBJETIVOS ESPECÍFICOS

- Proteger la información de la Entidad que se maneja dentro de los recursos físicos y digitales que son de uso de los funcionarios, contratistas, terceros y, en general, de los colaboradores de la Entidad.
- Establecer las directrices que los colaboradores deben conocer, apropiar y aplicar de frente al uso adecuado que garantice los niveles óptimos de seguridad y privacidad de la información.
- Concientizar a los usuarios de frente al uso de la información que se maneja en los recursos físicos y digitales entregados para la realización de sus funciones.
- Proteger la información que se encuentra en documentos que reposan en los puestos de trabajo de los funcionarios de la Entidad.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

Esta política se aplica a cualquier tipo de información de la Cámara de Representantes que se crea, utiliza, procesa, almacena y/o elimina, en los puestos de trabajo, equipos de cómputo, unidades de

almacenamiento extraíble, contenedores físicos de información, y que se encuentran en cualquier tipo de formato físico y digital. En tal sentido, la política tiene como propósito llegar a todos los colaboradores, funcionarios, contratistas, terceros, externos, aprendices, practicantes, y toda aquella persona con que tenga relación con la Entidad.

4. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
NTC-ISO / IEC 27001:2013	2013	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
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.

Escritorio Limpio: En términos de seguridad de la información, hace referencia a la protección de la información con el propósito de reducir los riesgos de acceso no autorizado, pérdida, daño o divulgación no autorizada de información durante todo su ciclo de vida, y frente a los recursos físicos y digitales de uso de los funcionarios de la Entidad.

6. DESCRIPCIÓN DE LA POLÍTICA

Todo el personal de la Cámara de Representantes, incluyendo a funcionarios, contratistas y terceros que interactúan con la información de la Entidad deben apropiar las mejores prácticas de seguridad y privacidad de la información que permitan reducir los riesgos de acceso no autorizado, daño, pérdida o divulgación no autorizada de la información que crean, utilizan, procesan, almacena, en sus puestos de trabajo, equipos de cómputo, unidades de almacenamiento extraíble, contenedores físicos de información, de toda aquella información física y digital , con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información.

La presente política debe aplicarse tan pronto como se sospeche que los sistemas de información o los datos están en funcionamiento, o están realmente afectados por un evento adverso que probablemente conduzca a un incidente de seguridad.

Un "incidente de seguridad en la gestión de la información" es un evento adverso que ha causado o tiene el potencial de causar daños a los bienes, la reputación y/o a colaboradores, contratistas y terceros de la Entidad. La gestión de incidentes se ocupa de la intrusión, el compromiso y el mal uso de la información y recursos de información, y la continuidad de los sistemas y procesos de información críticos. Puede enfocarse inicialmente a los servicios de tecnología, pero también se aplica a los registros en papel, las cartas y cualquier otra forma los datos se almacenan o procesan.

6.1. LINEAMIENTOS

6.1.1 SOBRE EL ESCRITORIO LIMPIO

- La información crítica de negocio que se encuentra en cualquier medio físico y/o. digital debe tener las medidas de protección necesaria para salvaguardas su confidencialidad, integridad y disponibilidad, entre ellas, guardar la información en contenedores seguros no cuando se requiera, y en especial, cuando la misma sea desatendida por los usuarios.
- No exponer, publicar, divulgar, o dejar a la vista información sensible que contenga datos de la Entidad o información de datos personales o cualquier información que se considere importante para la Cámara de Representantes. Así mismo, éstos deben quedar fuera del alcance de terceros sin autorización y/o supervisión.
- Evitar el acceso no autorizado, la pérdida o daño de la información que se utiliza en los puestos de trabajo y/o en los dispositivos digitales.
- Evitar el uso de líquidos o elementos que puedan generar un riesgo frente a la información física y digital.
- Los dispositivos de almacenamiento electrónico deben ser protegidos contra acceso no autorizado y estar almacenados en lugares seguros.
- No registrar credenciales de acceso en papeles ni en ningún tipo de documento físico ni digital de fácil acceso y sin la protección adecuada para ello.
- El usuario debe guardar todo material que contenga información sensible de la Entidad en cualquier momento que su puesto de trabajo quede desatendido o cuando finalice su jornada laboral.
- Mantener bajo llave la información sensible y elementos de valor que le han sido entregados.

6.1.2 SOBRE EL EQUIPO DE COMPUTO

- Los equipos de cómputo deben tener implementados mecanismos de protección ante el acceso no autorizado.
- Asegurar físicamente los equipos de cómputo portátiles mediante cables de seguridad para evitar la pérdida o robo de dichos dispositivos.
- El usuario es responsable de realizar el bloqueo, el cierre de sesión o el apagado del equipo de cómputo que tiene asignado cuando se encuentra ausente, su equipo se

encuentra desatendido o finaliza su jornada laboral y/o su uso.

- Los usuarios no tienen permitido realizar traslados de los elementos de cómputo que tiene asignados, a excepción de los equipos portátiles que tienen asignado para el desarrollo de sus funciones.
- El escritorio del equipo de cómputo no debe tener información sensible que sea de fácil acceso.
- Se deben establecer los mecanismos necesarios para realizar el bloqueo de pantalla de los equipos de cómputo por inactividad en un tiempo razonable.

6.1.3 SOBRE DISPOSITIVOS DE REPRODUCCIÓN DE INFORMACIÓN

- Los equipos de reproducción de información como impresoras, fotocopiadoras, multifuncionales, etc. deben estar ubicados en áreas de acceso controlado, con el propósito de evitar el uso no autorizado.
- Los documentos que contienen información sensible se deben retirar de las impresoras inmediatamente.
- En los casos que sea posible, configurar los dispositivos de manera que utilicen mecanismos de autenticación con el fin de evitar el acceso no autorizado, y el controlar que el creador de la información sea quien tiene el derecho a la reproducción de la ésta.

6.1.4 SOBRE OTROS ELEMENTOS Y DISPOSITIVOS

- Se debe realizar evaluaciones de riesgos de frente al uso de dispositivos y tecnologías que permitan realizar copias de la información de la Entidad, tales como teléfonos, impresoras, fotocopiadoras, escáneres y cámaras, entre otros.

7. RESPONSABLES

- El **Responsable de la Seguridad de la Información** es responsable de velar por el cumplimiento de la presente política y realizar el seguimiento y la actualización de los lineamientos que aplican mantenerla vigente.
- El **Responsable de la Oficina de Planeación y Sistemas** deben implementar los controles tecnológicos necesarios que apliquen para el cumplimiento de la Política.
- Los **Usuarios** son personalmente responsables de cumplir con las políticas, leyes y regulaciones aplicables en todo momento.

8. INCUMPLIMIENTO

El incumplimiento de la Política de Escritorio Limpio 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.

10. CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
1	16/12/2021	• 05/11/2020 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