DINÁMICA Desarrollo Institucional & de Procesos	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**

1. Objetivo:

Establecer los lineamientos y procedimientos que garanticen las medidas necesarias para proteger la información contra acceso no autorizado, la divulgación, la duplicación, la modificación, la destrucción, la pérdida, el robo o mal uso que pueda ocurrir en forma intencional o accidental de la información digital y los de ciberseguridad.

2. Alcance:

La Política, es aplicable a todos los procesos, áreas, y a toda la población como empleados, contratistas y terceros que usen información que sea propiedad de Dinámica y de las entidades a las cuales les prestamos los servicios de consultoría. Y su acceso debe limitarse a lo estrictamente imprescindible para el desarrollo de las funciones para cada puesto de trabajo.

No se permitirá la utilización de los medios electrónicos corporativos para uso personal, ni utilizar la información después de haber finalizado el vínculo con Dinámica.

3. Normatividad:

3.1 En este contexto, la presente tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrada en el artículo 20 de la misma.

3.2 LEY 527 DE 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

3.3 LEY 1266 DE 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

3.4 LEY 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

3.5 LEY 1273 DE 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.

3.6 LEY 1712 DE 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.

3.7 RESOLUCIÓN 500 DE MARZO 10 DE 2021 DEL MINTIC: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

3.8 DECRETO 338 DE MARZO DE 2022 DEL MINTIC: Se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital NTC ISO/IEC 27001 DE 2013 Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.

4. Definiciones:

4.1 Dato Personal:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

4.2 Dato sensible:

Información que afecta la intimidad del titular o cuyo uso indebido pueda generar algún inconveniente

4.3 Encargado del Dato:

Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, realice tratamiento de Datos

4.4Responsable del Dato:

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 Datos

4.5 Titular del Dato:

Persona natural o jurídica, pública o privada, cuya información sea almacenada en las bases de datos de Dinámica, y sea objeto de tratamiento.

4.6 Tratamiento:

Cualquier operación o conjunto de operaciones sobre los Datos, como la recolección, almacenamiento, uso, circulación o supresión.

4.7 Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

4.8 Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física

4.9 Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

5. Principios para el Tratamiento de Datos:

De acuerdo con la Ley 1581 de 2012, el tratamiento de datos personales debe regirse por los siguientes principios:

- Legalidad
- Finalidad
- Libertad
- Veracidad o calidad
- Transparencia
- Acceso y circulación restringida
- Seguridad
- Confidencialidad

6. Políticas de Seguridad de la Información

6.1 Confidencialidad

- Todos los datos personales serán tratados bajo estricta confidencialidad.
- Se firmarán acuerdos de confidencialidad con empleados y terceros que manejen datos personales.

6.2 Control de Acceso

- Se implementarán medidas para garantizar que solo personal autorizado acceda a la información personal.
- Se usarán contraseñas seguras, autenticación de múltiples factores y restricciones por roles.

6.3 Integridad de la Información

- Se realizarán copias de respaldo (backups) de la información periódicamente.
- Se llevarán a cabo controles para prevenir alteraciones o pérdidas de información.

6.4 Disponibilidad

- La organización garantizará que los datos personales estén disponibles para su tratamiento, cuando sea requerido por ley o por el titular.

6.5 Seguridad Física y Lógica

- Se protegerán físicamente los dispositivos y servidores donde se almacene información.
- Se implementará software antivirus, firewalls y actualizaciones permanentes.

6.6 Gestión de Incidentes

- Se tendrá un procedimiento para notificar y gestionar incidentes de seguridad que afecten los datos personales.

7. Responsables De Implementar y hacer seguimiento al cumplimiento de esta política

7. 1 Dirección: Asegurara el adecuado manejo de la información y tratamiento de los datos personales, cumpliendo lo establecido por la ley.

7. 2 Todos los Servidores y Colaboradores de Dinámica en el marco de sus funciones y obligaciones.

Elaborado febrero 15 de 2022