Para garantizar un adecuado manejo de la seguridad informática de **SEGURIDAD THOR LTDA,** se han establecido las siguientes directrices:

1. Seguridad sobre la asignación y el uso de los recursos

- Los equipos de cómputo y manejo de seguridad informática, que están asignados a empleados de la Empresa, están configurados con una contraseña de ingreso, con la cual el usuario debe ingresar.

- El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe asegurar que se cumpla esta política. Además, todo el personal deberá informar a sistemas o funcionario asignado, sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.

- Todo el personal tendrá una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo sólo son para uso interno y externo de la Organización.

- El uso de internet queda reservado solo para las actividades de trabajo que así lo requieran. En general se restringe el acceso mediante el uso de contraseña en el administrador de contenidos de Internet Explorer. Únicamente se da acceso a las páginas que por las actividades que desarrolla la Empresa se deben consultar.

2. Sobre la seguridad de la información

- Semanalmente se realizan Back-Ups de la información de la Empresa que se maneja en medio electrónico.

- Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.

- Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.

- Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.

- El responsable del sistema de información designará periódicamente nuevas contraseñas tanto para el acceso a las sesiones Windows como para el acceso a los programas.

- A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades:

  - ✓ Actualizar su base de firmas de virus (actualización de la lista de amenazas)
  - ✓ Búsqueda de virus (análisis del equipo)
  - ✓ Eliminación de virus si fue detectado.

- Para el uso de USB, discos, programas, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además, los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

3. Sobre el mantenimiento y buen uso de la infraestructura

- Una vez al año se realizara una revisión a los equipos para detectar desperfectos y dar así mantenimiento.

- Periódicamente se realizará una limpieza física a toda la infraestructura del equipo de cómputo por parte del personal de sistemas.

- Toda actividad elaborada por el equipo de sistemas o funcionario asignado debe estar debidamente documentada para efectos de trazabilidad de las actividades realizadas.

4. **Sobre las medidas disciplinarias, a los infractores del sistema de seguridad de tecnología de la información.**

- En caso de detectarse y comprobarse uso mal intencionado del sistema de seguridad de tecnología de la información por parte de los empleados, la Empresa aplicará las medidas sancionatorias necesarias, de acuerdo con lo establecido en el procedimiento de administración de personal, el reglamento interno de trabajo, el procedimiento de Seguridad informática y demás normatividad legal vigente.

JAIRO ANTONIO ASCANIO LOPEZ

Gerente General y Representante Legal

Bogotá, 15 de febrero de 2022

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción del Cambio	Solicitado por
01	17.07.2018	Documento Nuevo	Gerencia
02	15.02.2022	Revisión del Documento	Gerencia

AUTORIZACIONES

ELABORO	REVISO	APROBO
Lider SIG	SUBGERENCIA	GERENTE GENERAL