La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de WIMAX ZOMAC SAS con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

WIMAX ZOMAC SAS, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

• Minimizar el riesgo de los procesos misionales de la entidad.

• Cumplir con los principios de seguridad de la información.

• Cumplir con los principios de la función administrativa.

• Mantener la confianza de los funcionarios, contratistas y terceros.

• Apoyar la innovación tecnológica.

• Implementar el sistema de gestión de seguridad de la información.

• Proteger los activos de información.

• Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

• Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del WIMAX ZOMAC SAS

• Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

• Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del WIMAX ZOMAC SAS y la ciudadanía en general.

Se define el objetivo, alcance, criterios, etc. Se debe planear mínimo una auditoría al mes para el procedimiento.

Director de Infraestructura, debe revisar diariamente la página del MINTIC, ingresando con el usuario y contraseña al portal de las URLs suministradas por estos.

Se procede a descargar el archivo actualizado para ingresarlo al servidor FTP de la compañía y este es entregado al CIO para su carga al servidor FTP.

Se ingresa por medio del software FileZilla a la dirección IP del servidor con el usuario y contraseña.

Se ingresa al directorio ftp_mintic

Se sobrescriben los archivos: paginas_prohibidas_mintic.txt y coljuegos.txt

El técnico del CIO procede a actualizar los listados de URL del MINTIC y Coljuegos en el servidor FTP de la compañía