1.- Es responsabilidad de los usuarios propietarios de cada carpeta el contenido de la información de cada uno de los archivos existentes en las mismas, así como su manejo, la depuración y el orden.

2.- Para la creación de una nueva carpeta compartida, ésta deberá de solicitarse al área de T.I. con los parámetros de nombre, usuarios que tendrán acceso y el tipo de permiso en la misma, mediante una solicitud de soporte en la intranet posterior a su creación, el propietario de la misma es el responsable de su contenido.

3.- No ésta permitido tener archivos en los servidores, de manera temporal, permanente o de paso de las siguientes características:

- ***Pornografía, en cualquiera de sus expresiones (películas, videos, caricaturas, etc).***
- ***Música, en cualquiera formato.***
- ***Fotografías, que no tengan ningún vínculo laboral***

4.- Queda prohibido grabar archivos en carpetas del sistema operativo del equipo asignado y/o del servidor al que se tenga permitido el acceso.

5.- El acceso a un archivo ó carpeta, deberá solicitarse a él área de T.I. mediante una solicitud de soporte en la intranet incluyendo la información necesaria para el acceso a la misma, de igual forma, por el mismo medio, se buscará la autorización de acceso del dueño de la información a la que se pretende ingresar.

6.- El personal de T.I. tiene la autorización de borrar archivos, carpetas y programas en los diferentes servidores y equipos de la red de datos GIM, que estén provocando inconsistencias en espacio y el buen funcionamiento, que no estén autorizados, y/o licenciados.

7.- Todo el material (información, aplicaciones, archivos) que sea recibido a través de cualquier medio de almacenamiento de información, así como todo el material descargado de Internet, recibido por correo o desde cualquier otra computadora o red de computadoras, DEBE ser revisado (escaneado) contra cualquier virus y/o programa destructivo ANTES de ser cargado en nuestra red de datos GIM. La omisión del proceso de escaneo que cause la infección de un equipo o red de datos GIM será sancionada según las acciones disciplinarias establecidas por el comité de vigilancia interna.

8.- El usuario no podrá alterar ó borrar archivos y/o configuraciones de servidores a los que tiene permitido el acceso.

9.- No se podrán integrar a la red de datos GIM cualquier tipo de dispositivo o equipos personales para el intercambio de información propiedad de Grupo GIM.

10.- La información propiedad del grupo GIM y que tenga que compartirse con proveedores, clientes y/o autoridades gubernamentales por necesidades de negocios ó requerimientos específicos, deberán de enviarse por medio de correo electrónico, OneDrive de Microsoft, ya que estos medios tienen configurada la seguridad de encriptación TLS y/o SFTP que tiene seguridad de encriptación SSH a través de clave publica/privada, de acuerdo a lo mencionado en el documento **Lineamiento de Seguridad de la Información en red de datos GIM.**

11.- La información que tenga que recibirse de proveedores, clientes y/o autoridades gubernamentales por necesidades de negocios ó requerimientos específicos, deberán de recibirse por medio de correo electrónico, OneDrive de Microsoft, ya que estos medios tienen configurada la seguridad de encriptación TLS y/o SFTP que tiene seguridad de encriptación SSH a través de clave publica/privada, de acuerdo a lo mencionado en el documento **Lineamiento de Seguridad de la Información en red de datos GIM.**

12.- El área de TI del corporativo de grupo GIM, podrá revisar a fondo un equipo y apoyarse en herramientas de software y hardware necesario, ya sea gratuito y/o licenciado, así como de un proveedor externo, cuando un director del corporativo ó subsidiaria del grupo GIM lo solicite debido a evidencias de falta de ética del empleado.