**Objetivo**

Establecer criterios que permitan mantener un entorno informático seguro y controlado para el desarrollo de las actividades de la organización.

1. **Acceso Físico**

La Empresa destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de IT.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor de este o el superior responsable o el personal de IT.

1. **Protección Física** 
   1. Data Center

El Data Center deberá:

• Tener una puerta de acceso que permanecerá cerrada para favorecer el control del uso de los recursos de cómputo.

• Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la gerencia de Tecnología.

• Recibir mantenimiento mensual.

• Estar libre de contactos e instalaciones eléctricas en mal estado

• Aire acondicionado. Mantener la temperatura a 21 grados centígrados.

• Respaldo de energía redundante.

• Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

• Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

* 1. Infraestructura

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

El resguardo de los equipos de cómputo deberá quedar bajo el área de Tecnología contando con un control de los equipos que permita conocer el inventario de los mismos.

1. **Instalaciones de equipos de cómputo**

La instalación del equipo de cómputo quedará sujeta a los siguientes lineamientos:

• El Área de Tecnología, deberá contar con un plano actualizado de telecomunicaciones.

• Las instalaciones eléctricas y de telecomunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

• Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

• En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

1. **Control**

• El administrador de infraestructura deben llevar un control total de los recursos de cómputo y licenciamiento.

• El Administrador de Infraestructura es el responsable de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

1. **Respaldos**

• Las Bases de Datos de Las Empresas serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

• Los respaldos no pueden guardarse en el mismo servidor que se respalda.

• Los respaldos deben ser almacenados en un lugar seguro y distante del sitio de trabajo.

• Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por La Empresa en “La Nube” (Google Drive), deberá realizar una sincronización continua de la información importante de Las Empresas. Los respaldos serán responsabilidad absoluta de los usuarios

• El Administrador de Infraestructura no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

1. **Recursos de los usuarios** 
   1. Uso

• Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y Red de Las Empresas, de acuerdo con las políticas que en este documento se mencionan.

• Los usuarios deberán solicitar apoyo al área de Tecnología ante cualquier duda en el manejo de los recursos de cómputo de La Empresa.

• El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la Empresa, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

* 1. Derechos de Autor
* Queda prohibida la extracción de información de la compañía con otros fines que no sean estrictamente laborales y en beneficio de la entidad.

• No está autorizada la descarga de Internet de programas informáticos no autorizados por La Gerencia o la Gerencia de Tecnología de GI.

* No está autorizada la instalación de aplicaciones que requieran licencia sin contar con una, exceptuando las versiones demo.

• No se tolerará que un empleado realice copias no autorizadas de programas informáticos.

• No se tolerará que un empleado cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.

• Si se encuentran aplicaciones sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

• Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

• Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

1. **Vigencia y Revisión:**

La presente política queda vigente desde el momento de su aprobación y debe revisarse en un período de 12 a 18 meses.