

# POLÍTICA DE SEGURIDAD, INGRESO Y USO DE SERVICIOS DE DATA CENTER

## PRIMERO: PROPÓSITO Y ALCANCE

Con la finalidad de fortalecer nuestras medidas de seguridad, integridad, continuidad operativa y eficiencia en la atención de nuestros clientes, se establece la siguiente normativa unificada para el acceso y uso del servicio de alojamiento (*Colocation*) en los Data Centers y sitios técnicos habilitados de Gtd.

## SEGUNDO: POLÍTICAS Y PROTOCOLOS DE INGRESO

- **Programación previa:** Todo acceso al edificio o sala Data Center realizado por clientes, contratistas o terceros autorizados debe ser programado y aprobado previamente.
- **Anticipación y Portal Web:** La solicitud de ingreso debe generarse con al menos 1 hora de anticipación a través del portal de clientes habilitado: <https://extranet.grupogtd.com/>, ingresando con el usuario y contraseña entregados por su ejecutivo comercial. Ante dudas o inquietudes, el cliente puede contactar al Área de Atención Comercial mediante el teléfono **800 390 800** o el correo electrónico **soportet@grupogtd.com**.
- **Identificación en la Recepción:** Al arribar al Data Center, toda persona debe identificarse en la recepción presentando su cédula de identidad o pasaporte vigente. No son válidas las credenciales ni documentos como la licencia de conducir.
- **Inducción Data Center:** Antes del primer ingreso del cliente a una instalación y previo al acceso a la sala de Racks se le dará una inducción de forma audiovisual o verbal para el correcto uso del servicio.
- **Credencial y Tarjeta de Acceso:** Se entregará una credencial de acceso que debe permanecer visible en todo momento durante la visita. Asimismo, se otorgará una tarjeta de acceso individual que limitará el tránsito exclusivamente a las áreas específicas donde el cliente tiene sus equipos instalados. Esta tarjeta debe ser devuelta obligatoriamente al abandonar las dependencias.
- **Aforo Máximo:** Se autoriza un máximo de 3 personas por visita/solicitud.
- **Aviso de Salida:** Al finalizar las labores, se debe informar la salida a través de los teléfonos habilitados al costado del acceso de cada sala. Un operador del Data Center revisará el estado de la instalación y procederá al cierre con llave del rack respectivo.

## TERCERO: POLÍTICAS DE INGRESO, INSTALACIÓN Y RETIRO DE EQUIPOS

- **Solicitud de ingreso:** El ingreso a las dependencias del Data Center se realizará mediante un Formulario de Solicitud de ingreso (habilitado en <https://extranet.grupogtd.com/>), documento que respaldará cada acceso, equipamiento ingresado, cantidad de asistentes y acción a realizar.
- **Declaración en Solicitud:** Todo ingreso, retiro o cambio de equipamiento debe ser declarado en el formulario de la solicitud de ingreso (**Opción: Ingresa equipos Sí / No**).
- **Documentación y Guías de Despacho:** Todo ingreso o retiro de equipos debe realizarse respaldado por su respectiva Guía de Despacho, entregada a un operador. Para todo retiro de

equipos, el cliente deberá informar al operador asignado, quien verificará la información en la documentación de despacho correspondiente al egreso.

- **Consumo Eléctrico:** Se debe informar de manera previa el consumo eléctrico estimado de los equipos a instalar, para la correspondiente validación técnica por parte del personal del Data Center.
- **Kits de Montaje y Cables de Poder:** Todo equipo a instalar debe contar con su kit de montaje completo y sus cables de poder correspondientes. Todos los cables de poder deben ser revisados y aprobados previamente por personal de Gtd antes de su energización para prevenir cortocircuitos o fallas eléctricas.
- **Conexiones Eléctricas:** Queda estrictamente prohibida la instalación y conexión en cadena de PDU (*Daisy Chain*), salvo autorización expresa del personal del Data Center.
- **Coordinación Preventiva (24 Horas):** Para nuevas instalaciones, cambios de volumen o retiros masivos, se recomienda gestionar el acceso con al menos 24 horas de anticipación, asegurando la asignación de un operador dedicado para asistencia.
- **Especificaciones Técnicas e Identificación:**
  - Los equipos deben instalarse orientando la fuente de poder y el flujo de aire caliente hacia el pasillo caliente.
  - Todo equipo destinado a rack compartido debe **someterse a pre-test previo a su montaje.**
  - Todos los equipos deben estar correctamente rotulados e identificados por el cliente.
- **Dispositivos Periféricos:** Se recomienda no dejar instalados dispositivos periféricos de forma permanente (adaptadores USB, discos externos HDD, mouse, teclados) en los equipos alojados, a fin de evitar desconexiones accidentales por manipulación inadvertida.
- **Retiro de Pallets y Embalajes:** Para nuevas instalaciones que involucren pallets o gran volumen de embalaje, el cliente es responsable de retirarlos íntegramente de las dependencias del Data Center.

#### CUARTO: POLÍTICAS DE SEGURIDAD Y CONTROL DE SALAS

- **Sustancias y Elementos Prohibidos:** Queda estrictamente prohibido fumar, ingresar con alimentos, líquidos, tabaco o derivados, explosivos, armas, sustancias químicas o drogas ilegales.
- **Tránsito y Limpieza:** Queda prohibido entorpecer el libre tránsito en pasillos y dejar basura, embalajes o accesorios de equipos fuera de los recipientes habilitados para su disposición.
- **Cuidado de la Infraestructura:** Queda estrictamente prohibido dañar, intervenir o adulterar la infraestructura de las salas (sensores, pintura, tuberías, escalerillas, cableado, etc.).
- **Prevención de Incendios:** Se prohíbe mantener elementos inflamables dentro, sobre racks o sobre el hardware instalado (cajas de cartón, papeles, bolsas de plástico, embalajes). Si se detecta la presencia de estos materiales, el área de Data Center gestionará su retiro inmediato a través del ejecutivo comercial o responsable del rack.
- **Registro Audiovisual:** Se prohíbe tomar fotografías o grabar videos en la totalidad de las dependencias del Data Center.
- **Permanencia en Sala:** Por seguridad y salud ocupacional, se sugiere no permanecer más de 3 horas continuas dentro de la sala limpia. En caso de requerir mayor tiempo, se recomienda salir al exterior al menos 5 minutos.
- **Responsabilidad del Cliente:** Es responsabilidad exclusiva del cliente gestionar la

autorización para el ingreso de terceros o contratistas externos, la adecuada manipulación de sus trabajos en los racks, así como mantener actualizados sus datos de contacto (comerciales, correos y teléfonos).

## QUINTO: PROTOCOLO DE ACCESO URGENTE / EMERGENCIA

En caso de requerir acceso no programado de urgencia: el cliente debe presentarse directamente en la recepción del Data Center, donde un operador asistirá en la tramitación e ingreso inmediato.

## SEXTO: SERVICIOS Y EQUIPAMIENTO HABILITADO EN SALAS

Gtd pone a disposición del cliente en sus salas técnicas los siguientes recursos complementarios para facilitar su operación:

- Carros multi-periféricos.
- Enchufes de servicio.
- Red WiFi Corporativa.
- Teléfonos internos de sala.
- Asistencia de Operadores NOC y Servicio de Manos Remotas.
- Salas de Armado y Preparación (disponibles en sedes Lídice I, Lídice II y Panamericana).

## SÉPTIMO: CONTINUIDAD OPERATIVA Y CONTROL TÉRMICO (BLANK PANELS)

Para asegurar la continuidad operativa y el correcto flujo de aire y la integridad climática de la sala blanca, el cliente deberá instalar obligatoriamente **Blank Panels** (paneles ciegos) en todos los espacios vacíos (unidades de rack libres) de su gabinete.

En caso de detectarse fugas o filtraciones térmicas durante las inspecciones preventivas de Gtd, se solicitará por correo electrónico la autorización para intervenir el rack e instalar los paneles faltantes. De no obtener respuesta a una segunda notificación, Gtd queda facultada para emitir las multas estipuladas en el Contrato del servicio.

## OCTAVO: ACTUALIZACIÓN Y MODIFICACIÓN NORMATIVA

Para garantizar la mejora continua y adaptar la seguridad a nuevos estándares, Gtd se reserva el derecho de actualizar o modificar esta política. Las versiones vigentes estarán siempre publicadas y accesibles en el portal oficial: <https://www.gtd.cl/datacenter>.