transpack®

GLOBAL
MOBILITY

Predio Goodpark - Nave 5.
Colectora Ruta 2 Km. 39,5 - Ing. Allan, Buenos Aires.
T: (5411) 3221 6900 - **F:** (5411) 3221 6901
info@transpack.com.ar - **www.transpackinternational.com**

Política de ciberseguridad

1. Propósito

El propósito de esta política es establecer pautas y procedimientos para proteger los activos digitales y la información confidencial de la organización contra amenazas cibernéticas, garantizando la integridad, confidencialidad y disponibilidad de los datos.

2. Alcance

Esta política se aplica a todos los empleados, contratistas y terceros que acceden, utilizan o administran los recursos tecnológicos y la información de la organización.

3. Responsabilidades

- La dirección ejecutiva será responsable de proporcionar los recursos y el apoyo necesarios para implementar y mantener esta política.
- El equipo de seguridad de la información supervisará y ejecutará las medidas de seguridad cibernética.
- Todos los empleados y partes interesadas deberán cumplir con esta política y seguir las directrices establecidas.

4. Protección de Activos Digitales

- Todos los dispositivos y sistemas informáticos deberán estar protegidos con contraseñas seguras y actualizadas regularmente.

- Se implementará software antivirus y antispyware en todos los dispositivos de la red.

- Se utilizarán firewalls y filtros de contenido para proteger contra intrusiones y ataques maliciosos.

- Se realizarán copias de seguridad de datos regularmente y se almacenarán en ubicaciones seguras fuera del sitio.

5. Gestión de Acceso

Predio Goodpark - Nave 5.
Colectora Ruta 2 Km. 39,5 - Ing. Allan, Buenos Aires.
T: (5411) 3221 6900 - **F:** (5411) 3221 6901
info@transpack.com.ar - **www.transpackinternational.com**

- Se asignarán permisos de acceso basados en el principio de mínimo privilegio, limitando el acceso solo a las personas que necesiten la información para llevar a cabo sus funciones.

- Se implementará un proceso de gestión de identidad y acceso para crear, modificar y revocar cuentas de usuario según sea necesario.

6. Concientización y Formación

- Se proporcionará formación en seguridad cibernética a todos los empleados para aumentar la conciencia sobre las amenazas y mejores prácticas de seguridad.

- Se realizarán simulacros de phishing y otras actividades de sensibilización para educar a los empleados sobre cómo reconocer y evitar ataques cibernéticos.

7. Incidentes de Seguridad

- Se establecerá un proceso de gestión de incidentes para detectar, investigar y responder a posibles violaciones de seguridad.

- Se notificarán los incidentes de seguridad al equipo de seguridad de la información de manera oportuna para que puedan tomar medidas correctivas adecuadas.

8. Revisión y Actualización

- Esta política será revisada y actualizada regularmente para reflejar los cambios en la tecnología y las amenazas cibernéticas.

- Se llevarán a cabo revisiones periódicas de cumplimiento para garantizar que esta política se esté aplicando de manera efectiva en toda la organización.