POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente política establece los principios fundamentales para proteger la información y los activos tecnológicos de PROCOLLECT CONTACT CENTER S.A., asegurando su disponibilidad, confidencialidad e integridad, así como el estricto cumplimiento de la normativa legal vigente, en especial la Ley N° 19.628 sobre Protección de la Vida Privada.
Esta política ha sido aprobada por el Directorio y refleja el compromiso de la organización con la seguridad de la información, la protección de los datos personales, el cumplimiento normativo y la continuidad operacional.
Aplica a todos los colaboradores, proveedores y terceros que accedan, procesen, almacenen o custodien información de la empresa o de terceros en su poder.

PRINCIPIOS RECTORES

1- Valor de la Información
La información, especialmente aquella que contiene datos personales, es un activo estratégico de la organización. Su tratamiento debe realizarse con el más alto nivel de protección y conforme a los principios establecidos en la Ley N° 19.628.

2- Responsabilidad Compartida
La seguridad de la información es una responsabilidad transversal. Todos los miembros de la organización, sin distinción de rol o jerarquía, deben actuar con diligencia y cumplir esta política y la normativa vigente sobre privacidad y protección de datos.

3- Compromiso con la Confianza y Continuidad
PROCOLLECT CONTACT CENTER S.A. se compromete a proteger la información confiada por sus clientes, colaboradores y terceros, garantizando:

- Su uso legítimo y proporcional.
- La confidencialidad, integridad y disponibilidad.
- La continuidad del negocio.

4- Acceso Controlado y Justificado
El acceso a la información se autoriza solo en función del principio de mínimo privilegio. Se otorgarán permisos exclusivamente a quienes lo requieran para sus funciones, conforme a criterios de necesidad, proporcionalidad y trazabilidad.

5- Confidencialidad de la Información
Está estrictamente prohibido divulgar, ceder o transferir información de carácter confidencial o datos personales, salvo cuando:

- Exista consentimiento expreso del titular.
- La ley lo autorice expresamente.
- Sea necesario para el cumplimiento de obligaciones contractuales, en cuyo caso deberá garantizarse la confidencialidad, seguridad y trazabilidad del tratamiento.

6- Cumplimiento Legal y Regulatorio
Se implementarán controles para asegurar el cumplimiento de todas las leyes y regulaciones aplicables en materia de protección de datos personales, ciberseguridad y privacidad, incluyendo:

- Derecho de los titulares a acceder, rectificar, eliminar u oponerse al tratamiento de sus datos personales.
- Obligación de informar a los titulares sobre la finalidad del tratamiento.
- Medidas técnicas y organizativas para evitar accesos no autorizados.

7- Supervisión y Control de Recursos Tecnológicos
La empresa podrá monitorear o auditar el uso de dispositivos corporativos o personales, exclusivamente en los siguientes casos:

- Con autorización del Comité de Riesgo Tecnológico y Seguridad de la Información.
- Por motivos fundados, como sospechas de vulneraciones a esta política o amenazas a la seguridad o integridad de los sistemas de la empresa.
- Garantizando siempre el respeto a la vida privada y derechos fundamentales de las personas, en conformidad con la Ley N° 19.628.

8- Gobernanza y Coordinación de la Seguridad
El Comité de Seguridad de la Información establecerá directrices estratégicas. Su implementación corresponderá a las unidades de negocio, bajo la coordinación del Oficial de Seguridad de la Información (CISO), quien será responsable de velar por el cumplimiento de esta política y la legislación aplicable.

9- Fiscalización y Medidas Disciplinarias
El incumplimiento de esta política será considerado como una falta grave, con posibles sanciones administrativas y contractuales, sin perjuicio de otras acciones legales que correspondan.