Rosario,
Septiembre 2022

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Entendiendo que en **PREVI S.R.L** los datos de nuestros clientes, nuestro personal y base de datos de clientes y potenciales clientes utilizadas en el desarrollo y ejecución de campañas de ventas de tangibles e intangibles y demás activos de la información son esenciales para la prestación de nuestros servicios, tomamos el compromiso de operar en un ambiente propicio que garantice la **Seguridad de la Información**, entendiendo por ello asegurar laConfidencialidad, Integridad y Disponibilidad de la información y la **Ciberseguridad**, entendiendo por ello proteger los activos de la información, abordando amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.

Por lo tanto, **nos comprometemos** a:

1. Asegurar la Disponibilidad, Integridad y Confidencialidad de la información, al prestar nuestros servicios.

2. Desarrollar actividades de formación y concienciación, paratodo el personal de Previ S.R.L, relativas a Seguridad de la Información y Ciberseguridad.

3. Analizar permanentemente los Riesgos y gestionar los mismos estableciendo los controles necesarios .

4. Difundir la presente Política a todaparte interesada, comunicando asínuestros valores y compromiso conforme a la Seguridad de la Información.

5. Definir Procedimiento de Gestión deContinuidad del Negocio, a fin de recuperar las funciones críticas y cumplir los objetivos de Previ S.R.L, ante la ocurrencia de eventualidades.

Rosario,
Septiembre 2022

6

Establecer acuerdos de confidencialidad de la informaciónen contratos de personal y colaboradores de Previ S.R.L, extendiendo la responsabilidad al uso de recursos informáticos fuerade las dependencias de las instalaciones de Previ S.R.L.

7

Cumplir con los requsitos del negocio y con las obligaciones legalesy reglamentarias pertinentes.

8

Implementar, mantener y certificar ante organismos internacionales un Sistema de Gestión de Seguridad dela Información, basado en la norma ISO 27001:2013, a fin de gestionar los riesgos, lograr la mejora continua y garantizar el crecimiento integral denuestra organización.

9

Ejecutar acciones de ciberseguridada fin de minimizar riesgos, tales como:

-Desarrollar planes de Formación de ciberseguridad.

-Utilización adecuada y modificaciónperiódica de contraseñas.

-Actuación prudente y preventiva delos equipos y dispositivos electrónicos, la navegación porinternet y el correo electrónico.

-Prueba y actualización de los planesde contingencia.

-Instalación y actualización automática de software de protección.

-Asignación de permisos de acceso ala información.

-Realización periódica de copias deseguridad.

-Control periódico y auditado de los Proveedores Externos de Servicios Informáticos

- Segregación de los entornos de desarrollo, testeo y producción.
- Los datos utilizados en entornos de desarrollo nunca serán los mismos datos utilizados en producción.
- Realizar controles de introducción de código malicioso en entornos de desarrollo.

Flavia Vignolo
Directora Comercial
PREVI S.R.L

Romina Prezzavento
Directora Operativa
PREVI S.R.L