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 la **Confidencialidad, Integridad y Disponibilidad** de la información y la **Ciberseguridad**, protegiendo los activos de la información, abordando amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados

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

2. Desarrollar actividades de **formación y concienciación**, para todo 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 toda parte interesada, comunicando así, nuestros **valores y compromisos** conformes a la Seguridad de la Información.

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

6. Establecer **acuerdos de Confidencialidad** de la información en contratos de **personal y Proveedores** de Previ S.R.L, extendiendo la responsabilidad al uso de recursos informáticos fuera de las dependencias.

7. Cumplir con los **requisitos del negocio** y con las **obligaciones legales** y reglamentarias pertinentes.

8. **Implementar, mantener y certificar** ante organismos internacionales un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001, con el fin de gestionar los riesgos, lograr la mejora continua y garantizar el crecimiento integral de nuestra organización.

9. Ejecutar acciones de **ciberseguridad** con el fin de minimizar riesgos, tales como:
-Realizar **controles** de introducción de **código malicioso** en entornos de desarrollo.
-Realizar **backups** sistemáticos y periódicos.
-Revisiones regulares de **acceso**.
- S**egregación de los entornos** de desarrollo, testeo y producción.
-Realizar actividades periódicas de **análisis de vulnerabilidades**.

Flavia Vignolo
Directora Comercial

Romina Prezzavento
Directora Adm, y Finanzas

Rev 02
29/07/2024