Nuestra "Política de Seguridad de la Información" parte de la base de que la "información" y los datos que la generan, cualquiera que sea la forma en que se recibe, se almacena, comunica y comparte, los activos físicos y lógicos, así como la privacidad de los datos tratados, debe ser y estar siempre protegida contra usos y accesos indebidos con el fin de garantizar el cumplimiento de la legislación y compromisos contractuales aplicables, la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones y oportunidades de negocio.

Así pues, como parte específica de nuestra "**POLÍTICA EMPRESARIAL**", la Dirección de **PROTECTUM SEGURIDAD**, establece la siguiente:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Conocer y gestionar los riesgos operacionales y estratégicos en materia de seguridad de la información para que permanezcan en niveles aceptables y razonables de seguridad para **PROTECTUM SEGURIDAD** Incluyendo:

- La protección de la confidencialidad de la información relacionada con las AAPP, clientes y otras Partes Interesadas, garantizando la correcta implantación de sistemas de control, custodia y comunicaciones internas y externas empleados en la gestión de dicha información.
- La inadmisibilidad de situaciones que puedan exponer a **PROTECTUM SEGURIDAD** a la violación de la Legislación en materia de seguridad de la información existente.
- Garantizar el derecho a la protección de los datos personales de todas las personas físicas que se relacionan con nosotros; asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, de conformidad con lo dispuesto en la legislación sobre protección de datos personales y garantía de los derechos digitales.
- Establecer y comunicar a todo el personal pautas de uso de los sistemas de información disponibles, especialmente en lo relativo a las "Tecnologías de Información" (TI). El personal será formado, informado y asumirá la responsabilidad de la seguridad de la información que se le encomiende, según sea relevante para el desempeño de su trabajo.
- Las decisiones en materia de seguridad de la información se adoptarán en función de los riesgos y oportunidades identificados en cada momento, incluyendo las posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
  - Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.

Compromisos:

- Desarrollar e implantar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma internacional ISO 27001.
- Establecer, planificar, revisar y hacer seguimiento de objetivos e Indicadores en el ámbito de la Seguridad de la Información.
- Dotar los recursos (humanos y materiales) necesarios para su consecución.
- Asumir la responsabilidad de la seguridad de la información en los procesos y actividades que se desarrollan en nuestras instalaciones.
- Mantener, aplicar y revisar periódicamente el Sistema de Gestión de Seguridad de la Información, mejorando su eficacia con la aplicación de acciones derivadas del análisis del desempeño y la información obtenida en las auditorías y en las revisiones periódicas.
- Colaborar activamente con la cadena de suministro para fomentar el avance en sus compromisos y estándares de seguridad de la información.

Ernesto Martín Zuasti
Director General