La presente Política de Seguridad de la Información tiene como objetivo el cumplimiento de la exigencia del **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el **Esquema Nacional de Seguridad** (**ENS**) e **ISO/IEC 27001:2022**, en el ámbito de la Administración Electrónica, que en su artículo 12 establece la obligación a las Administraciones Públicas y a los proveedores de servicios de las Administraciones públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

GESTIÓN CUATROCIENTOS S.L, tiene como misión prestar servicios de desarrollo de aplicaciones para administraciones públicas así como otros servicios de consultoría y formación.

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de toda la información gestionada.

Se ha diseñado una Política de Seguridad de la Información cuyos objetivos principales son:

- Proteger mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.
- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.
- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- Especificar los efectos que conlleva el incumplimiento de la Política de Seguridad en el ámbito laboral.
- Evaluar los riesgos que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes.
- Formar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar y cumplir la legislación en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc, que afecte a los activos de la entidad.
- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.