POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

MONENTIA, S.L., dedicada a la consultoría tecnológica y al desarrollo de sistemas de información, ha implantado un Sistema de Gestión de la Seguridad de la Información basado en los requisitos de la norma ISO 27001:2022 con el objetivo de garantizar que todos los activos y recursos de tecnología de la información se utilicen y gestionen de una manera que proteja su confidencialidad, integridad y disponibilidad y destinado a asegurar la continuidad de las líneas de negocio, minimizar los daños y maximizar el retorno de las inversiones y las oportunidades de negocio y la mejora continua.

La Dirección de **MONENTIA, S.L.,** mediante la elaboración e implantación del presente Sistema de Gestión de Seguridad de la Información adquiere los siguientes compromisos:

Desarrollar soluciones y servicios conformes con los requisitos legislativos, identificando para ello las legislaciones de aplicación a las líneas de negocio desarrolladas por la organización e incluidas en el alcance del SGSI.

- Establecer y cumplir los requisitos contractuales con las partes interesadas.
- Construir y mantener la confianza de los clientes, empleados y reguladores.
- Garantizar la confidencialidad de los datos médicos de los asegurados.
- Proporcionar programas de formación y concienciación en seguridad de la información para todos los empleados y otras partes interesadas.
- Prevenir y detectar cualquier virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento de acuerdos contractuales con organizaciones especializadas.
- Realizar evaluaciones de riesgo de seguridad de la información para identificar e implementar controles para mitigar el impacto de los riesgos identificados.
- Desarrollar y mantener planes de continuidad del negocio y recuperación ante desastres.
- Establecimiento de las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
- Promover una cultura de mejora continua en la gestión de la seguridad de la información e implementar mejoras basadas en el análisis de incidentes, auditorías y revisiones periódicas.
- Actuar en todo momento dentro de la más estricta ética profesional.
- Asegurar que el acceso y uso de los sistemas de información se realice de manera segura y conforme a las políticas establecidas.
- Mantener la reputación de la marca con respecto a la seguridad de los datos.
- Gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.
- El personal de la organización participará en la gestión de los incidentes relacionados con los servicios y gestión de la seguridad de la información, con objeto de restablecer con la máxima celeridad posible los niveles normales de operación de los servicios y minimizar los impactos adversos de dichos incidentes en la organización.
- Asegurar la protección de los derechos de propiedad intelectual.
- Establecer periódicamente un conjunto de objetivos e indicadores, que permitan a la dirección llevar a cabo un adecuado seguimiento de los niveles de servicio ofrecidos y las actividades de gestión.
- La dirección se compromete a proporcionar los recursos necesarios para mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI).

Fdo. Director General

Rev.00