



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La organización, empresa dedicada a la promoción, desarrollo, construcción y gestión de proyectos y servicios, ha decidido implantar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, proteger a ésta de un amplio grupo de amenazas 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 **la organización** es consciente de que la información es un activo que tiene un elevado valor para la Organización y requiere por tanto una protección adecuada.

La Dirección de **la organización**, establece como objetivos de base, punto de partida y soporte de los objetivos y principios de la seguridad de la información los siguientes:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización.
- La protección de los derechos de propiedad intelectual.
- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.
- La formación y capacitación para la seguridad de la información.
- El registro de las incidencias de seguridad.
- La gestión de la continuidad del negocio.
- La gestión de los cambios que pudieran darse en la empresa relativos a la seguridad

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

- Desarrollar productos 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 Sistema de Gestión de la Seguridad de la Información.
- Establecimiento y cumplimiento de los requisitos contractuales con las partes interesadas.
- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento de planes de formación.
- Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento acuerdos contractuales con organizaciones especializadas.
- Gestión de la continuidad del negocio, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- 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.
- Actuar en todo momento dentro de la más estricta ética profesional.

Esta Política proporciona el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información así como para establecer y revisar los objetivos del Sistema de Gestión de Seguridad de la Información, siendo comunicada a toda la Organización a través de la página web y su publicación en paneles informativos, siendo revisada anualmente para su adecuación y extraordinariamente cuando concurren situaciones especiales y/o cambios sustanciales en el Sistema de Gestión de Seguridad de la Información, estando a disposición público en general.

Dirección

Madrid, 20 de Enero de 2023