ENETIC, es consciente y asume su compromiso con la seguridad de la información según las normas de referencia ISO 27001, ISO 27017 y Esquema Nacional de Seguridad categoría Media, así como con la protección de información personal según la norma ISO 27018. Por lo que la dirección de **ENETIC** establece los siguientes principios:

- Velar por garantizar la satisfacción de nuestros clientes, incluyendo las partes interesadas en los resultados de la empresa, en todo lo referente a la realización de nuestras actividades y su repercusión en la sociedad.
- Velar por garantizar la seguridad de la información de los sistemas de información de **ENETIC**, así como de los sistemas de información que dan soporte a los servicios prestados por **ENETIC** a sus clientes.
- Establecer objetivos y metas enfocados hacia la evaluación del desempeño en materia de seguridad de la información, así como a la mejora continua en nuestras actividades, reguladas en el Sistema de Gestión de Seguridad de la Información que desarrolla esta política.
- Cumplimiento de los requisitos de la legislación aplicable y reglamentaria a nuestra actividad, los compromisos adquiridos con los clientes y todas aquellas normas internas o pautas de actuación a los que se someta **ENETIC.**
- Mantenimiento de una comunicación fluida tanto a nivel interno, entre los distintos estamentos de la empresa, como con clientes.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Velar por la mejora continua del Sistema de Gestión Integrado que desarrolla esta política.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.

Para los servicios Cloud (IaaS), adicionalmente:

- Se identificarán los requisitos básicos de seguridad aplicables al diseño e implantación del servicio.
- Se tendrán en cuenta los riesgos provenientes del personal interno autorizado.
- Se securizarán los servicios multi-cliente (multi-tenancy) y aislamiento de clientes (incluyendo virtualización).
- Se controlará el acceso a activos del cliente por parte de personal propio.
- Se implementará autenticación fuerte para usuarios administradores.
- Se comunicará a los clientes la ubicación de los CPDs, y si así lo solicitan, los cambios en la infraestructura.
- Se implementará seguridad en todo el proceso de virtualización y se usaran herramientas certificadas.
- Se protegerá tanto el acceso como la información del cliente.
- Se gestionarán las cuentas de los clientes durante todo su ciclo de vida.
- Se comunicará a organismos a proveedores, Partners y organismos especializados (CERT) las brechas de seguridad y se compartirá información para ayudar en la investigación de ciberincidentes.
- Es política de **ENETIC** implementar, mantener y realizar un seguimiento del Sistema de Gestión de Seguridad de la Información.

Estos principios son asumidos por la Dirección de **ENETIC**, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad de la Información.

Fdo: José Martí Herrero Dirección: Ronda narciso Monturiol nº 7, 46980 Paterna, Valencia	Firmado por ***5663** JOSE MARTI (R: ****4942*) el día