Aprobación y entrada en vigor

Texto aprobado el día 18 de Agosto de 2020 por Jose Martí, Director General de **ENETIC**.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hora hasta que sea reemplazada por una nueva versión.

Declaración Política de Seguridad

ENETIC define la presente Política de Seguridad, de carácter obligatorio para todos sus empleados, teniendo un objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Uno de los objetivos es establecer las directrices que garanticen la seguridad de la información en **ENETIC** a un nivel adecuado según el nivel de riesgo de los activos y las necesidades y recursos de esta organización.

Este documento debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve **ENETIC** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la Información serán:

- Velar por la seguridad de la información, en sus distintas dimensiones.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos, para reducir o eliminar los riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos, productos y servicios.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos.
- Realizar una adecuada gestión de incidentes que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.

Incumplimiento

El incumplimiento de la Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Terceras partes

Las empresas y organizaciones externas que con ocasión de su colaboración con **ENETIC** para la prestación de un servicio, accedan o gestionen activos de información de **ENETIC** o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos de **ENETIC**, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a **ENETIC** sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de **ENETIC** que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a **ENETIC**. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de **ENETIC** a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas de **ENETIC**. Específicamente, cualquier equipo conectado a la red corporativa de **ENETIC** debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de **ENETIC** desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

ENETIC se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

Firmado por JOSE MARTÍ el día 25/08/2020 con un certificado emitido por AC Representación