POLITICA DE SEGURIDAD DE LA INFORMACIÓN NEXUS ENERGÍA, S.A.

Barcelona, 31 de julio de 2019
Director General de Nexus Energía, S.A.

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN 4
5. NORMATIVA EXTERNA APLICABLE 4
6. NORMATIVA INTERNA APLICABLE 5

1. INTRODUCCIÓN

Nexus Energía, S.A. (Nexus, en adelante) es una comercializadora de energía eléctrica y gas natural y, por tanto, nos definimos como una empresa de servicios. En consecuencia, además de los empleados que configuran Nexus, nuestros principales activos son de naturaleza intangible y por tanto están formados por información confidencial, datos personales y know-how, entre otros.

Por ello, la protección y la seguridad de la información que manejamos es clave, asumiendo el compromiso de organizar nuestros procesos de acuerdo al establecimiento y aplicación de un marco interno de regulación que nos permita proteger y asegurar que la información y los datos personales de nuestras partes interesadas sean tratados de manera apropiada.

2. OBJETIVO

El objetivo de esta política es proporcionar orientación de cómo Nexus afronta la gestión de la seguridad de la información de acuerdo con los requisitos del negocio y las normas aplicables. Para ello, se utiliza como marco de referencia la norma ISO 27001, complementada con la norma ISO 27002. Esta política se desarrolla en diversa normativa interna que guía a todos los empleados en el cumplimiento de las normas ISO referidas, las leyes y reglamentos sobre la protección de datos personales, las obligaciones contractuales adquiridas y en la aplicación de las mejores prácticas en materia de seguridad de la información y protección de datos.

En todos los niveles de Nexus se velará por la aplicación real y efectiva de las medidas de prevención y control previstas en esta política y en toda aquella normativa interna que la desarrollan.

Las actuaciones que se derivan de la aplicación del marco normativo buscan la consecución de los objetivos estratégicos definidos en la organización en el ámbito de un proceso de mejora continua y en línea con los requisitos de seguridad de la información contenidos en la norma ISO 27001.

Los objetivos de Nexus en materia de seguridad están alineados con los de negocio, dando prioridad al cumplimiento de las obligaciones legales que sean aplicables a la actividad desarrollada, preservando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y ofreciendo a las partes interesadas la confianza sobre la adecuada gestión de los riesgos.

3. ALCANCE

El alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) a certificar bajo normas ISO 27001 es el siguiente:

Los sistemas de información que dan soporte a la comercialización de electricidad y gas en los procesos de Tramitación, Lectura, Facturación y Gestión de Cobros.

4. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN

La dirección de Nexus se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la organización, así como a demostrar el liderazgo y compromiso respecto a este, a través del nombramiento de un Responsable de Seguridad y la constitución del Comité de Protección de Datos y Seguridad de la Información.

Dicho Comité tiene una función de coordinación, acompañamiento y apoyo a toda la organización y en especial a quienes recaen las funciones de control. Coordina una función preventiva del modelo de prevención descrito en las políticas de protección de datos y de seguridad de Nexus. Es un órgano con poderes autónomos de iniciativa y de control, reportando al Consejo de Administración de Nexus a través de su Comisión de Auditoría. Asimismo, tiene la responsabilidad de:

- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Comunicar y difundir las políticas relacionadas con el SGSI dentro de la organización y a las partes interesadas.
- Asegurar que el SGSI consigue los resultados previstos.
- Promover la mejora continua del SGSI.
- Revisión de la política siempre que se produzcan cambios significativos o como mínimo una vez al año.

5. NORMATIVA EXTERNA APLICABLE

NORMATIVA EXTERNA DE REFERENCIA

- Reglamento (UE) 2016/679 de 27 de abril Reglamento General de Protección de Datos (RGPD).
- Ley orgánica 3/2018 de protección de datos de carácter personal.
- Real Decreto Legislativo 1/1996 de la Ley de Propiedad Intelectual.
- Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad y su modificación por el Real decreto 951/2015 de 23 de octubre (e las relaciones con el sector público).
- Código Penal.

MARCOS NORMATIVOS EXTERNOS DE REFERENCIA

- ISO 27001.
- ISO 27002.

6. NORMATIVA INTERNA APLICABLE

Esta política se desarrolla en diversa normativa interna, entre las que se destacan:

- **Política Detallada de Seguridad de la Información**: con el objetivo de proporcionar una guía detallada para todas las personas que conforman la organización sobre cómo debe gestionarse la seguridad de la información. Contiene una descripción de los elementos clave, tanto humanos como organizativos, tecnológicos y documentales, que Nexus aplica para proteger la información, y especialmente los datos de carácter personal, evitando que se produzcan incidentes de seguridad que los pongan en peligro.

- **Política de Protección de Datos:** su objetivo es establecer las directrices a seguir en materia de protección de datos. Esta política contiene una descripción de los elementos clave, tanto humanos como organizativos, tecnológicos y documentales, que NEXUS aplica para proteger los datos de carácter personal, evitando que se produzcan vulneraciones de los derechos y libertades de los interesados.

- **Normas de uso de los recursos Tecnologías de la Información y Comunicación:** con el objetivo de regular el uso de los recursos TIC por parte de sus usuarios, tanto internos como externos y garantizar la seguridad de éstos, así como de los datos personales e información confidencial que albergan.

- **Procedimiento de gestión de incidentes de seguridad de la información:** con el objetivo de definir las acciones a realizar en la gestión, valoración y notificación, en su caso, de un incidente de seguridad que comporte una potencial violación de datos personales.