



Windar renovables

# Política de seguridad de la información

## Windar renovables

### Marco de actuación

Los activos que manejamos de forma habitual y los sistemas tecnológicos que nos ofrecen acceso a la información, constituyen para las compañías y sociedades de Grupo WINDAR, activos críticos y fuentes prioritarias de innovación y desarrollo sostenible en una economía en el camino de la digitalización y seguridad de la información a escala mundial.

Desde Grupo WINDAR visualizamos como en la actualidad los hábitos y la cultura de nuestras personas y partes interesadas están cambiando constante, motivados por la aparición e influencia de las nuevas tecnologías y el enorme volumen de información que se recibe, creando un panorama marcado por tendencias sociales que se ajustan a estos cambios vividos. La preocupación actual de clientes, inversores, personas trabajadoras y otras partes interesadas por el planeta y el cambio climático debido a las últimas crisis y conflictos, está impactando en las comunidades y organizaciones transformando las formas de trabajo hacia nuevos modelos donde los sistemas de información y su seguridad son clave para el crecimiento.

En esta línea, observamos la aceleración constante hacia la adopción de nuevas e innovadoras tecnologías por parte de todos los sectores industriales, las cuales, vienen a actuar como un elemento catalizador para el desarrollo sostenible y un cambio en el crecimiento de la compañía. En paralelo, el enorme aumento del volumen de datos y repositorios de información que se manejan en las compañías y sociedades de Grupo WINDAR y la gestión de los mismos, cobra un valor muy importante en la medida de que deben protegerse frente las amenazas e intrusiones, buscando soluciones para la seguridad y privacidad de todas nuestras partes interesadas.

El uso de mayor cantidad de dispositivos que comparten información o datos como resultado de la transformación digital y la expansión de los horizontes de internet que estamos viviendo, en primer lugar está creándose una tendencia asociada a que la información se encuentre alojada en sistemas en la nube, o que las personas trabajadoras y los activos digitales se encuentren localizados cada vez más fuera de las instalaciones, como se venía haciendo de forma tradicional. En segundo lugar los ciberataques están ocasionando importantes daños convirtiéndose en un desafío ligado a la obligación de disponer de nuevas infraestructuras de internet seguras para afrontar nuevas amenazas. Estas situaciones demandan la necesidad de que la seguridad de la información sea más flexible y adaptable al entorno actual.

### Declaración

Por todo ello, es prioritario y un firme compromiso de la Dirección de las compañías y sociedades de Grupo WINDAR, garantizar la protección en términos de confidencialidad, integridad y disponibilidad, tanto de los sistemas como activos de información, estableciendo todos los controles y medidas de seguridad necesarias.

Estos controles incluyen los datos tratados de los profesionales de Grupo WINDAR, así como de cualquier otra parte interesada con la que nos relacionemos durante nuestras relaciones comerciales y de negocio, los activos físicos y lógicos, así como, las infraestructuras críticas necesarias para el mantenimiento de los servicios prestados por la organización.

A la hora de desarrollar las medidas de seguridad y ciberseguridad orientadas a mitigar y reducir los riesgos, Grupo WINDAR como parte de su proceso de debida diligencia, contribuirá al cumplimiento de los principios fundamentales del Pacto Mundial de las Naciones Unidas a los que nos hemos adherido, así como al cumplimiento de los ODS de las Naciones Unidas, ayudando a crear infraestructuras resilientes, promoviendo una industrialización inclusiva y sostenible, mejorando la eficiencia energética y fomentando la innovación. Es posible también que internet se convierta en un elemento responsable con el medio ambiente, garantizando que el acceso sea equitativo a la red, se impulse la inclusión digital y la promoción de la responsabilidad social.

Para fortalecer este compromiso, la Alta Dirección comunica esta Política de Seguridad de la información a todos sus profesionales y a terceros. Esta Política, se alinea con el modelo de gestión internacional fundamentado sobre la norma ISO 27001 con el ánimo de alcanzar los más altos niveles de seguridad de la información, estableciendo los principios generales y medidas que regirán todas las actuaciones en esta materia en todas las localizaciones en el mundo donde realiza sus operaciones.

## Windar renovables

### Despliegue de la política

Las compañías y sociedades de Grupo WINDAR en todo el mundo se comprometen a promover y fomentar los siguientes principios de actuación, los cuales regirán sus actividades en materia de seguridad de la información de forma corporativa:

- ⇒ Liderar la mejora continua del sistema de gestión de la compañía integrando la Seguridad de la Información a través de la implementación de la norma internacional ISO 27001 en todas las localizaciones donde realiza sus operaciones.
- ⇒ Diseñar un conjunto de Políticas específicas de seguridad sobre cada uno de los controles más relevantes mediante unas “**Normas básicas de Seguridad de la Información**” que se comuniquen y rijan el comportamiento y manera de actuar de todas las personas trabajadoras y otras partes interesadas relacionadas con Grupo WINDAR.
- ⇒ Crear una cultura de responsabilidad de todo el equipo humano sobre el cumplimiento de la presente Política de SI, así como del resto de Políticas y normas específicas que la desarrollen y las reglamentación vigente a todos los niveles de la compañía,
- ⇒ Garantizar que tanto los sistemas como los activos de información disponibles, sean utilizados únicamente para los propósitos necesarios y autorizados, estableciendo los mecanismos y sanciones necesarias en caso de incumplimiento.
- ⇒ Desarrollar y aplicar medidas que permitan identificar y proteger los sistemas y activos de información frente a accesos no autorizados, modificaciones, comunicaciones o destrucciones intencionadas o fortuitas.
- ⇒ Establecer objetivo en materia de SI que apoyen la consecución de los resultados de negocio.
- ⇒ Asegurar que se dispone de los recursos y activos necesarios que permitan asegurar la protección de la información interna y externa, así como de los datos personales.

Para abordar de forma efectiva todos estos compromisos que acabamos de detallar, Grupo WINDAR establece los principios, medidas y actuaciones específicas detallados en esta Política.

### Comité de seguridad

Grupo WINDAR desarrolla todas sus actuaciones al amparo del modelo de cumplimiento, la legislación vigente, el Código ético y el Sistema de gobernanza y sostenibilidad de la compañía, garantizando que se proporciona el soporte y la gestión necesaria para respetar todos estos requerimientos. Para ello, se ha constituido un Comité de Seguridad de la Información, como máximo órgano interno fundamental para la toma de decisiones en esta materia, así como, para:

1. Velar por el cumplimiento de la Política y normas de SI establecidas.
2. Identificar y comunicar las responsabilidades en materia de SI a todo el personal, incluyendo los términos y condiciones de empleo en los acuerdos contractuales de trabajo.
3. Formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes, que hayan cometido una violación a la Política de SI.
4. Proteger y preservar adecuadamente todos los activos pertenecientes a la compañía y asegurar el acceso a los sistemas de información únicamente al personal autorizado.

## Windar renovables

### Sobre concienciación y sensibilización

- Concienciar y sensibilizar al personal y partes interesadas relevantes sobre el cumplimiento de la Política de SI, las normas de SI y las medidas que afectan al desarrollo de sus funciones, así como las expectativas depositadas sobre ellos en esta materia, a través de la ejecución de campañas periódicas de formación e información sobre eventos SI.
- Identificar las necesidades de formación e información sobre nuevas tecnologías y habilidades, e impartirlas a través de los programas formativos periódicos de la compañía.

### Sobre riesgos de SI para la continuidad del negocio

- Definir los roles y responsabilidades adecuados que permitan la implementación de un Plan de Tratamiento del Riesgo y la evaluación de su efectividad, asegurando que se reducen los riesgos identificados.
- Garantizar la continuidad de los servicios prestados considerados esenciales por la compañía y la continuidad de los procesos de negocio, aplicando controles y planes de contingencia que minimicen la materialización de riesgos críticos.

### Sobre SI en la relación con partes externas

- Trasladar la Política de SI y nuestros compromisos a proveedores y subcontratistas, así como a terceros con los que la compañía se relaciona, o bien que participan y colaboran en la SI, evaluando su eficacia periódicamente.
- Garantizar que los proveedores y subcontratistas u otras partes interesadas conocen y cumplen esta Política, de acuerdo con su rol en el momento que traten con información de la compañía o sus clientes.
- Hacer uso de acuerdos de confidencialidad o no divulgación para toda la información que debe protegerse, almacenarse y conservarse y activos a utilizar, incluyendo el tratamiento de los datos de carácter personal.

### Sobre configuración y mantenimiento de la seguridad

- Determinar las configuraciones de seguridad, respaldo de la información, cifrado, controles de acceso, normas de conexión a redes, seguridad física, uso de dispositivos BYOD, que son necesarias para el uso de los mismos por parte de los usuarios.
- Garantizar la administración y gestión de las plataformas y servicios vinculados al tratamiento de información, asegurando la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.
- Realizar tareas de mantenimiento periódico que permitan asegurar que los equipos mantienen la configuración de seguridad definida y que se encuentran protegidos frente a amenazas de índole físico.
- Proteger adecuadamente los equipos frente a amenazas externas como temperatura, humedad, polvo u otras amenazas.

### Sobre el acceso y uso de la información

- Proteger adecuadamente la información almacenada, procesada o accesible a través de cualquier dispositivo usado por usuarios. Tanto los documentos físicos, como los soportados en medios de almacenamiento extraíble, serán protegidos y controlados.
- Establecer mecanismos de clasificación, etiquetado y transferencia de la información interna y externa manejada, garantizando el acceso y distribución de la misma solo al personal autorizado a través de formas seguras.
- Utilizar sistemas y técnicas criptográficas para la protección de la información en base a la realización de análisis de riesgo, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

## Windar renovables

### Sobre el mantenimiento de los activos

- Identificar e inventariar todos los activos de información, incluyendo la sistemática adecuada para la eliminación segura de aquellos equipos que deban ser dados de baja o reutilizados.
- Mantener copias de seguridad de la información, software y sistemas para evitar pérdidas de documentación esencial.
- Desarrollar tareas de mantenimiento preventivo sobre los principales activos para garantizar su correcto estado y operación frente a riesgos de seguridad lógicos y físicos, incluyendo especialmente equipos de taller para actividades de mantenimiento frente a amenazas de índole físico (polvo, suciedad, humedad,...).

### Sobre los riesgos de seguridad física

- Implementar barreras físicas de acceso a las instalaciones de tratamiento de información, para evitar amenazas relacionadas con accesos no autorizados, físicas y ambientales como polvo, suciedad o humedad que afecten a los equipos.
- Controlar adecuadamente los accesos a las áreas seguras, registrando las visitas y estableciendo acuerdos de confidencialidad o necesidad de aplicar determinadas prácticas de seguridad.
- Definir sistemáticas para proteger los equipos cuando se usan fuera de las instalaciones (autorización, no dejar desatendido, conexión a redes externas, visualización, acceso no autorizado, otros).
- Implementar sistemáticas para la el uso y gestión de los soportes extraíbles y la eliminación segura de la información almacenada en dichos soportes una vez utilizada la misma.

### Sobre ciberseguridad y gestión de incidencias de SI

- Reportar todos los eventos de seguridad de la información y las vulnerabilidades asociadas a los sistemas de información, gestionándolas y siendo comunicadas de forma que se apliquen las acciones correctivas en el menor tiempo posible.
- Implementar un proceso y las herramientas tecnológicas necesarias que permitan dar respuesta a las incidentes de SI detectadas o reportadas por los usuarios, considerando las diferentes tipologías y criticidad de los incidentes identificados sobre la base del análisis de riesgos.
- Utilizar el conocimiento obtenido y los resultados del seguimiento de las incidencias de SI identificadas o reportadas, como base fundamental para el aprendizaje, fortalecimiento y mejora del sistema de gestión de SI.

### Sobre seguridad en relación a las personas

- Garantizar el derecho a la intimidad de todas las personas físicas relacionadas con la compañía mediante la protección de los datos personales tratados, limitando y gestionando los accesos a dicha información y otros activos asociados.
- Adoptar medidas de SI para evitar los accesos no autorizados a sistemas críticos que incluyan datos personales, así como, el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones.
- Establecer reglas y normas de SI que aseguren que,
  - a. Se hace un uso aceptable de la información puesta a su disposición así como otros activos asociados.
  - b. Se controla el acceso físico y lógico a la información y otros activos asociados.
  - c. Se proporcionan los derechos necesarios y adecuados de acceso a la información y otros activos asociados
  - d. Se mantiene el área de trabajo limpia y despejada.
- Implementar tecnologías y procedimientos de autenticación seguros basados en las restricciones de acceso a la información.