

# POLÍTICA DE CIBERSEGURIDAD



## ÍNDICE

<b>1. OBJETO</b> .....	3
<b>2. ÁMBITO DE APLICACIÓN</b> .....	3
<b>3. PRINCIPIOS BÁSICOS DE ACTUACIÓN</b> .....	4
<b>4. LÍNEAS DE ACTUACIÓN PRIORITARIAS</b> .....	4
<b>4.1. Resiliencia ante amenazas cibernéticas</b> .....	5
<b>4.2. Protección de la información sensible</b> .....	5
<b>4.3. Evaluación y mejora continua de la seguridad digital</b> .....	5
<b>4.4. Gestión eficiente de incidentes de seguridad</b> .....	5
<b>4.5. Fortalecimiento de la cultura de seguridad cibernética</b> .....	5
<b>5. MECANISMOS DE DIFUSIÓN, SUPERVISIÓN Y CONTROL DE LA POLÍTICA</b> .....	5
<b>6. APROBACIÓN Y VIGENCIA</b> .....	6

## 1. OBJETO

El **Consejo de Administración** de UMBRELLA GLOBAL ENERGY, S.A. (la “**Sociedad**”) tiene la responsabilidad de aprobar y actualizar las políticas corporativas que establecen las directrices para la actuación tanto de la **Sociedad** como de las sociedades integradas en el grupo (en adelante, “**Grupo UMBRELLA**” o el “**Grupo**”).

La presente Política de Ciberseguridad del **Grupo UMBRELLA** se fundamenta en el compromiso con la protección de datos, la prevención de ciberataques y la promoción de prácticas seguras en todos los aspectos de nuestras operaciones como empresa referente en energía solar fotovoltaica a nivel global.

El **Grupo UMBRELLA** reconoce la importancia fundamental de establecer compromisos que fortalezcan su propósito de proteger la información, garantizar la seguridad cibernética y promover prácticas seguras para proteger a las comunidades en las que opera, minimizando así cualquier impacto negativo en la seguridad digital y en la sociedad en general.

Esta Política de Ciberseguridad (en adelante, la “**Política**” o la “**Política de Ciberseguridad**”) tiene como propósito establecer los principios fundamentales de acción del **Grupo UMBRELLA** en lo que respecta a la seguridad digital, sin perjuicio de cumplir con otras normativas del **Grupo** que estén vigentes o se implementen en el futuro.

## 2. ÁMBITO DE APLICACIÓN

La presente **Política** resulta de aplicación a toda la plantilla del **Grupo UMBRELLA**.

Además, el ámbito de aplicación se extenderá, en la medida de lo posible, a todas aquellas terceras partes y al resto de los grupos de interés con los que el **Grupo** mantiene una relación de colaboración, como proveedores, colaboradores, accionistas y socios del **Grupo UMBRELLA**, incluyendo las empresas contratadas que actúen en nombre del **Grupo**, *joint ventures* y otras asociaciones equivalentes, siempre y cuando el **Grupo** asuma su control operacional. Para el resto de colaboradores, se evaluará el alineamiento entre sus políticas propias y las políticas del **Grupo UMBRELLA** y, en su caso, se promoverá la adhesión a la **Política de Ciberseguridad** del **Grupo UMBRELLA**.

### 3. PRINCIPIOS BÁSICOS DE ACTUACIÓN

El compromiso con la ciberseguridad del **Grupo UMBRELLA** se estructura en base a los siguientes principios fundamentales de acción, los cuales son aplicables a todas sus operaciones y se incorporarán en los procesos internos de toma de decisiones:

- **Liderar**, desde la dirección del **Grupo** y mediante el departamento de Tecnología de la Información, el compromiso de la organización con la ciberseguridad aportando los recursos necesarios.
- **Afianzar** un nivel apropiado de ciberseguridad en los sistemas de información y de telecomunicaciones, asegurando que posean un estándar adecuado de seguridad y resiliencia durante el desarrollo de las actividades y operaciones.
- **Establecer** procedimientos y responsabilidades que permitan una respuesta rápida, eficaz y ordenada ante incidentes de ciberseguridad adoptando las medidas de necesarias para que no lleguen a materializarse o minimizar los efectos.
- **Asegurar** un proceso de revisión y actualización continua del sistema de ciberseguridad para adecuarlo al entorno tecnológico cambiante y a las nuevas amenazas que van surgiendo.
- **Obtener** y mantener, en su caso, las certificaciones en ciberseguridad basadas en estándares internacionales.
- **Garantizar** que nuestra plantilla está debidamente informada y capacitada en materia de ciberseguridad con el fin de tener presentes las prácticas de trabajo y los procedimientos establecidos para el desempeño de sus funciones. Asimismo, requerir a proveedores y contratistas formación en la materia, previo al comienzo de la relación contractual efectiva.
- **Velar** por el cumplimiento del marco normativo del área de ciberseguridad, tanto de legislación vigente, como de reguladores o por compromisos contractuales.
- **Colaborar** con autoridades y organismos competentes para contribuir a la mejora de la ciberseguridad.

### 4. LÍNEAS DE ACTUACIÓN PRIORITARIAS

El **Grupo UMBRELLA** se compromete firmemente con la preservación de la seguridad digital y la protección de la información. En consecuencia, las líneas de acción prioritarias del **Grupo** son las siguientes:

#### 4.1. Resiliencia ante amenazas cibernéticas

Es de suma importancia comunicar a inversores y demás grupos involucrados que los riesgos relacionados con la seguridad cibernética pueden afectar la continuidad del negocio y su estrategia a corto, mediano y largo plazo. Por tanto, **Grupo UMBRELLA** llevará a cabo evaluaciones de riesgos y oportunidades en materia de ciberseguridad para desarrollar estrategias de mitigación y aplicar medidas correctivas.

#### 4.2. Protección de la información sensible

Es esencial implementar medidas que salvaguarden la información confidencial y minimicen los riesgos de ciberataques. Dado el impacto potencial de vulnerabilidades en la seguridad de la información, se priorizará la evaluación y mejora continua de los protocolos de seguridad para garantizar la protección de datos.

#### 4.3. Evaluación y mejora continua de la seguridad digital

Para comprender y reducir los riesgos cibernéticos, es crucial medir y analizar el impacto de las actividades en la seguridad digital. **Grupo UMBRELLA** establecerá planes de medición y reducción de riesgos cibernéticos mediante estrategias de mejora continua y planes de acción específicos.

#### 4.4. Gestión eficiente de incidentes de seguridad

La identificación temprana y la gestión efectiva de incidentes cibernéticos son cruciales para minimizar su impacto. Por ello, se priorizará la implementación de sistemas de detección de amenazas avanzadas y la creación de planes de respuesta a incidentes para garantizar una recuperación rápida y eficaz.

#### 4.5. Fortalecimiento de la cultura de seguridad cibernética

El fomento de una cultura organizacional consciente en seguridad cibernética es fundamental. **Grupo UMBRELLA** se dedicará a sensibilizar y capacitar a su personal en prácticas seguras de manejo de datos y sistemas, promoviendo así un entorno de trabajo seguro y resiliente frente a amenazas digitales.

### 5. MECANISMOS DE DIFUSIÓN, SUPERVISIÓN Y CONTROL DE LA POLÍTICA

El Departamento de Tecnología de la Información será responsable de supervisar, implementar, desarrollar y hacer cumplir la **Política de Ciberseguridad**. Contará con las facultades necesarias para liderar y controlar el funcionamiento, la efectividad y el cumplimiento de esta **Política**.

Este departamento se asegurará de que la **Política** se adapte a las cambiantes necesidades y circunstancias del **Grupo UMBRELLA**, y se aplicarán sanciones adecuadas de acuerdo con los sistemas disciplinarios vigentes en caso de incumplimiento de las medidas establecidas.

Se espera que todo el personal y aquellos que estén sujetos a esta **Política** cumplan con sus disposiciones en el ejercicio de sus responsabilidades. Asimismo, estará disponible para consulta en la página web corporativa del **Grupo UMBRELLA**: <https://umbrella-e.com/en/>.

## 6. APROBACIÓN Y VIGENCIA

Esta **Política de Ciberseguridad** ha sido aprobada por unanimidad por el **Consejo de Administración** de la Sociedad en fecha 13 de diciembre de 2023, entrando en vigor al día siguiente de su aprobación y manteniéndose vigente en tanto en cuanto no se apruebe su modificación.

## Control de versiones

EDICIÓN	FECHA	NATURALEZA DE LA EDICIÓN
V1	13/12/2023	1ª versión