POLÍTICA DE **CIBERSEGURIDAD**

DE SIEMENS GAMESA RENEWABLE ENERGY, S.A.

(Texto aprobado por acuerdo del Consejo de Administración de 16 de septiembre de 2021)

POLÍTICA DE CIBERSEGURIDAD

El Consejo de Administración de Siemens Gamesa Renewable Energy, S.A. (en adelante "**Siemens Gamesa**" o la "**Sociedad**" y el grupo de sociedades del que Siemens Gamesa es la sociedad dominante, el "**Grupo Siemens Gamesa**"), de conformidad con los artículos 33 de los Estatutos Sociales y 6 y 7.3 del Reglamento del Consejo de Administración, aprueba esta Política de Ciberseguridad de la Sociedad y del Grupo Siemens Gamesa, la cual se integra en sus normas de Gobierno Corporativo.

El objetivo de esta política es establecer los principios básicos y el marco general para el control y la gestión de los riesgos de Ciberseguridad a los que está expuesta Siemens Gamesa.

El marco de Ciberseguridad contiene las normas y regulaciones que establecen los requisitos organizativos, de procedimiento y técnicos para proteger los activos de información y los productos, soluciones y servicios de Siemens Gamesa frente a las ciberamenazas internas y externas, mejorando la capacidad de resiliencia de los negocios.

1. DEFINICIONES

- **Tecnología de la Información (IT):** Incluye todo el espectro de tecnologías de procesamiento de información, incluyendo software, hardware, tecnologías de comunicación y servicios relacionados, así como los procesos implementados para su soporte y gestión.
- **Tecnología de Operación (OT):** Incluye todo el hardware, software, procesos y políticas generadas como parte de los productos, soluciones y servicios, incluyendo: sistemas hardware y software como DCS, PLC, SCADA, sistemas electrónicos de detección, monitoreo y diagnostico en red, así como interfaces internas, humanas, de red, de software, de máquina o de dispositivo asociadas que se utilizan para proporcionar funciones de control, seguridad, fabricación u operación remota a procesos continuos, por lotes, discretos y de otro tipo.
- **Ciberseguridad:** La protección contra daños causados por ataques digitales contra la confidencialidad, integridad, disponibilidad, autenticidad, confiabilidad de la información y activos en el ciberespacio. Incluye y no se limita a la organización, la recopilación de recursos, procesos y estructuras para garantizar una seguridad de extremo a extremo en toda la cadena de suministro.

2. OBJETIVOS GENERALES

El objetivo general de la política de Ciberseguridad es definir y formalizar los marcos generales, que ayudarán a Siemens Gamesa a gestionar los riesgos de Ciberseguridad en dos dominios (colectivamente referidos como los "dominios de Ciberseguridad"):

- **Ciberseguridad IT:** Siemens Gamesa considera la información como uno de sus activos más importantes para el correcto y eficiente desarrollo de sus servicios y el cumplimiento de los objetivos y leyes corporativas, estableciendo así la Ciberseguridad IT como objetivo fundamental para garantizar que la información procesada sea precisa, está disponible a quién la requiera y no se revele sin autorización.
- **Ciberseguridad OT:** Siemens Gamesa es consciente de la evolución asociada a las ciberamenazas y las regulaciones de la Tecnología de Operación (OT), estableciendo la

Ciberseguridad OT como objetivo fundamental para apoyar a los clientes de Siemens Gamesa con la protección de la infraestructura crítica proporcionando ofertas de productos relevantes que respalden la seguridad durante todo el ciclo de vida del activo, adaptado para cumplir con la estrategia y los requisitos internos, legislativos y regulatorios.

3. PRINCIPIOS BÁSICOS

La política de Ciberseguridad se basa en los siguientes principios básicos:

- Proteger los activos de información y tecnológicos críticos de la compañía frente a las amenazas de ciberseguridad vigentes.
- Garantizar que los Sistemas de Información (IT) y Sistemas de Operación (OT) de Siemens Gamesa son capaces de implementar y mantener un nivel de seguridad y resiliencia adecuado basado en estándares relevantes y los requisitos de los clientes de Siemens Gamesa y siguiendo un enfoque basado en riesgos.
- Promover la implantación de mecanismos de seguridad y resiliencia adecuados para la gestión de los riesgos de seguridad a lo largo de la cadena de suministro.
- Sensibilizar a los empleados, contratistas y colaboradores sobre los riesgos de Ciberseguridad.
- Garantizar que los empleados, contratistas y colaboradores tengan los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarios para respaldar los objetivos de Ciberseguridad de la compañía.
- Promover las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación contra incidentes de Ciberseguridad.
- Proporcionar procedimientos y herramientas para adaptarse rápidamente a las condiciones cambiantes del entorno tecnológico y las nuevas amenazas.
- Garantizar el cumplimiento normativo asociado a las áreas de Ciberseguridad en toda la compañía.
- Colaborar con organizaciones, agencias gubernamentales y asociaciones relevantes para contribuir a la mejora global de la Ciberseguridad.

4. MODELO ORGANIZATIVO

4.1 Mandato y Gobierno

El Consejo de Administración de Siemens Gamesa ha decidido conferir el gobierno de Ciberseguridad al Consejero Delegado (CEO) con el soporte técnico del Director de Ciberseguridad (CCSO). El gobierno se realiza a través del Comité Holístico de Seguridad, presidido por el CCSO.

El CCSO tiene la autoridad para dar directivas y orientación, incluyendo el control y la coordinación de tareas en el ámbito de Ciberseguridad en los dominios de Ciberseguridad IT y Ciberseguridad OT.

De igual modo, en consulta con las áreas especializadas, definirá las regulaciones, estrategias y estándares técnicos vinculantes requeridos en toda la empresa para la Ciberseguridad IT y Ciberseguridad OT, así como los procesos, responsabilidades, organización, interfaces e instrumentos de control necesarios para asegurar su implantación y compatibilidad en toda la compañía.

4.2 Comité Holístico de Seguridad

El Comité Holístico de Seguridad (HSB) es el comité interdepartamental para las áreas de Siemens Gamesa (ON/OF/SE/IT/SEC/CO) que garantiza una colaboración estrecha, el intercambio de competencias y el compromiso con iniciativas y proyectos de seguridad comunes y alinea los programas y organizaciones individuales en temas de seguridad holística. El HSB tiene el mandato de:

- Garantizar la alineación entre las funciones de gobierno individuales.
- Decidir sobre propuestas comunes para proyectos e iniciativas relacionadas con la Seguridad Holística.
- Alinear y definir la estrategia común de Seguridad Holística.

El comité facilita desde una perspectiva holística la alineación en las estrategias y decisiones para soluciones de seguridad comunes y gestiona los requisitos de seguridad futuros del negocio, socios o partes interesadas externas, incluidas las perspectivas generales de Ciberseguridad, legislativas y del mercado global.

4.3 Modelo de Gobierno de Ciberseguridad

Con el fin de soportar los objetivos y principios de esta política, Siemens Gamesa implementa un Modelo de Gobierno de Ciberseguridad basado en una adecuada definición y asignación de funciones y responsabilidades de gobierno, gestión y operación, así como procedimientos, reglas, metodologías y herramientas que cubren ambos dominios de Ciberseguridad:

a) **Identificar** los riesgos, implementando estructuras y procesos para mantener y desarrollar capacidades de seguridad y que incluye los siguientes objetivos:
   - Promover la organización de Ciberseguridad con una visión holística en la compañía, basada en la identificación continua de riesgos y la reducción del nivel de exposición, asegurando el cumplimiento de los compromisos con los grupos de interés (accionistas/reguladores/clientes/proveedores).
   - Estandarizar y mantener un modelo de gobierno de Ciberseguridad basado en el riesgo, estándares claros y controles supervisados que optimicen la inversión de recursos.

b) **Proteger** de las amenazas, mejorando las medidas de protección de los activos digitales antes de materializarse el riesgo y que contempla como objetivo el desarrollo de las tecnologías de seguridad aplicables a la protección integral de los activos a lo largo de su ciclo de vida, su criticidad y el desarrollo de las amenazas.

c) **Detectar** amenazas mediante el uso de múltiples fuentes de inteligencia para poder gestionarlas de manera proactiva y que considera como objetivo aumentar las capacidades de detección de amenazas internas o externas con tecnologías y procesos avanzados.

d) **Responder** a los incidentes de Ciberseguridad, limitando su impacto en la compañía y que contempla como objetivo asegurar la continuidad de los servicios soportados por los activos que conforman la infraestructura tecnológica y digital de la compañía y reducir el impacto de los incidentes a través de protocolos corporativos.

e) **Recuperar** y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un evento de Ciberseguridad.