POLÍTICA DE **CIBERSEGURIDAD**

DE SIEMENS GAMESA RENEWABLE ENERGY, S.A.

(Texto aprobado por acuerdo del Consejo de Administración de 12 de septiembre de 2018)

POLÍTICA DE CIBERSEGURIDAD

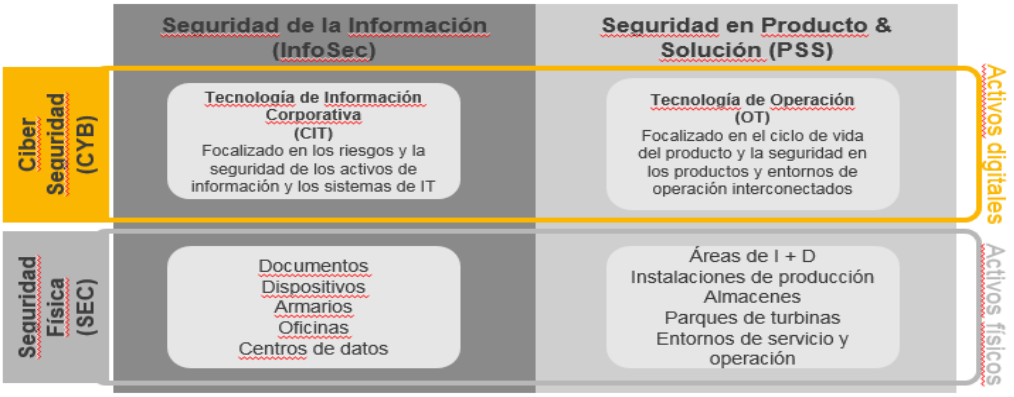
El Consejo de Administración de Siemens Gamesa Renewable Energy, S.A. (en adelante "**Siemens Gamesa**" o la "**Sociedad**" y el grupo de sociedades del que Siemens Gamesa es la sociedad dominante, el "**Grupo Siemens Gamesa**"), de conformidad con los artículos 529 ter de la Ley de Sociedades de Capital, 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.

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 y soluciones de Siemens Gamesa frente a las ciberamenazas internas y externas, mejorando la capacidad de resiliencia de los negocios.

1. DEFINICIONES

- **Tecnología de Información Corporativa (CIT):** Incluye todo el espectro de tecnologías de procesamiento de información, incluyendo software, hardware, tecnologías de comunicación y servicios relacionados.
- **Tecnología de Operación (OT):** Incluye hardware, software y sistemas de comunicación que forman parte de los productos y soluciones desarrollados por Siemens Gamesa. En general, incluye componentes de parque, sistemas de *backend* soportados por Siemens Gamesa y Sistemas de Control Industrial (ICS), siendo las más representativas las infraestructuras SCADA.
- **Ciberseguridad:** Cubre la seguridad del ámbito digital ("cibernético") a través de IT y OT. La ciberseguridad es complementaria al ámbito de la seguridad física, pero está estrechamente relacionada y en interdependencia con la misma.



2. OBJETIVOS GENERALES

El objetivo general de la política de Ciberseguridad es definir y formalizar los marcos generales, que ayudarán a Siemens Gamesa a mitigar los riesgos de ciberseguridad.

- **Seguridad de la Información**: 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 seguridad de la información como objetivo fundamental para garantizar que la información procesada sea precisa, está disponible a quién la requiera y no se revele sin autorización.
  Siemens Gamesa considera la serie ISO / IEC 27000 como estándar para este marco general.
- **Seguridad en Producto y Solución**: Siemens Gamesa es consciente de la evolución asociada a las ciberamenazas y las regulaciones de la Tecnología de Operación (OT) y Sistemas de Control Industrial (ICS), estableciendo la Seguridad en Producto y Solución como objetivo fundamental para garantizar que las infraestructuras críticas que soportan los productos y servicios de la compañía están protegidas.
  Siemens Gamesa considera la serie IEC 62443 como estándar para este marco general.

3. PRINCIPIOS BÁSICOS

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

- Garantizar que los sistemas de información, sistemas de operación y sistemas de comunicación de la compañía tengan un nivel de seguridad y resiliencia adecuado y apliquen los estándares más avanzados en los activos tecnológicos que respaldan la operación de infraestructuras críticas.

- Implementar las medidas de seguridad necesarias para proteger la confidencialidad, la integridad y la disponibilidad de la información y los sistemas de operación en función de su criticidad y los riesgos existentes, siguiendo un enfoque basado en el riesgo.

- Promover la implantación de mecanismos de seguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que prestan servicios a la compañía.

- Sensibilizar a todos los empleados, contratistas y colaboradores sobre los riesgos de ciberseguridad y garantizar que tengan los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarios para respaldar los objetivos de la compañía.

- Promover las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación contra incidentes y actividades del cibercrimen.

- 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 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 Seguridad de la Información y Seguridad en Producto y Solución.

De igual modo, en consulta con las áreas especializadas, definirá las regulaciones, estrategias y estándares técnicos vinculantes requeridos en toda la empresa para la Seguridad de la Información y Seguridad en Producto y Solución, 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 unidades de negocio (ON/OFF/SE) y áreas corporativas (IT/CT/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, herramientas e información o sistemas de operación apropiados para diferentes dominios considerados como parte del sistema:

a) **Gobernar** e 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.