QuintasGroup
MANAGING POWER

Política de Seguridad de la Información

Quintas Group Policy

Doc. QG-POL-0009.SP

Índice

Control de Versiones

Fecha	Versión	Autor(es)	Notas
05/12/2023	01	Julia Obermoller	Nueva política creada
27/03/2025	02	Francisco Domínguez	Cumplimiento con los requisites de la Norma ISO 27001:2023, incluyendo el cambio climático.

Introducción

"La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos."

El propósito de esta Política de Seguridad de la Información es demostrar el compromiso de Quintas Energy con la protección de los activos de información y con la garantía de la resiliencia de sus operaciones frente a amenazas en constante evolución, en alineación con la norma ISO/IEC 27001:2023.

Esta política se aplica a todas las partes interesadas, tanto internas como externas, que participan en el manejo de la información en Quintas Energy. Se pondrán copias de esta política a disposición de las partes interesadas relevantes.

Esta política será revisada anualmente o tras cambios significativos, tanto internos como externos.

Quintas Energy se compromete a:

1. Operar un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme con la norma ISO/IEC 27001:2023
   Implementando un SGSI que:
   - Cumpla con los requisitos de la norma ISO/IEC 27001:2023.
   - Apoye la consecución de los objetivos estratégicos.
   - Esté integrado en todas las unidades de negocio y niveles de la organización.
   - Se encuentre documentado, mantenido y en mejora continua.
   - Evalúe si el cambio climático es un aspecto relevante en el contexto de la organización, e integre esta consideración en el SGSI.

2. Gobernanza, Riesgo y Cumplimiento
   Mantener un marco documental para identificar, evaluar, tratar y monitorizar los riesgos relacionados con la seguridad de la información, incorporando:
   - La Declaración de Aplicabilidad (SoA) para la selección, justificación y seguimiento de los controles aplicables.
   - El cumplimiento de los requisitos legales, reglamentarios y contractuales.
   - La inclusión de la gobernanza de la seguridad de la información de terceros y de la cadena de suministro.
   - La supervisión del desempeño de los proveedores y del cumplimiento de los requisitos del Sistema de Gestión Integrado (SGI).
   - Nota: Las partes interesadas relevantes pueden tener requisitos relacionados con el cambio climático. Quintas Energy incluye estas consideraciones en su análisis de partes interesadas.

3. Objetivos de Seguridad de la Información y Seguimiento
   Definir objetivos de seguridad de la información medibles y alineados con los objetivos empresariales, revisados anualmente y respaldados por:
   - Evaluaciones periódicas del desempeño.
   - Auditorías internas y mejora continua.
   - Revisiones por la dirección conforme al apartado 9.3 de la norma ISO/IEC 27001.

4. Protección y Clasificación de Activos
   Garantizar que todos los activos de información sean:
   - Inventariados y clasificados de acuerdo con su nivel de sensibilidad (confidencialidad, integridad y disponibilidad).
   - Etiquetados y gestionados conforme a los procedimientos documentados.
   - Accesibles únicamente por personal autorizado y según el principio de necesidad de conocimiento (need-to-know).

5. Formación y Concienciación
   Proporcionar programas periódicos de formación y concienciación con el fin de:
   - Fomentar una cultura sólida de seguridad.
   - Asegurar que todo el personal comprenda sus responsabilidades en la protección de la información.
   - Abordar amenazas nuevas y emergentes, tales como fraudes por ingeniería social (Social Engineering Fraud - SEF), phishing, ransomware, entre otros.

6. Seguridad en los Proveedores y Servicios Externalizados
   Aplicar controles de seguridad a lo largo de todo el ciclo de vida de los proveedores, incluyendo:
   - La aplicación de procesos de precalificación y diligencia debida en función del riesgo.
   - La exigencia de compromisos contractuales en materia de seguridad de la información.
   - La supervisión del desempeño de los proveedores y del cumplimiento de los requisitos del SGSI.

7. Continuidad del Negocio y Respuesta ante Incidentes
   Mantener planes sólidos para:
   - Garantizar la continuidad de las operaciones críticas ante interrupciones.
   - Responder, gestionar y aprender de los incidentes relacionados con la seguridad de la información.
   - Probar y mejorar regularmente los planes de continuidad y los procedimientos de respuesta ante incidentes.

8. Mejora Continua y Adaptación a Amenazas
   Adoptar un enfoque de mejora continua mediante:
   - La monitorización de amenazas nuevas y emergentes (por ejemplo, riesgos cibernéticos, vulnerabilidades relacionadas con el cambio climático).
   - La aplicación de un enfoque de mejora basado en el riesgo y orientado por datos.
   - La integración de las lecciones aprendidas en las actualizaciones del sistema y en las campañas de concienciación.

9. Gobernanza de la Información y Control Documental
   Garantizar que las políticas, procedimientos y registros documentados sean:
   - Controlados, revisados y aprobados conforme al Procedimiento de Control Documental de Quintas Energy (QG).
   - Accesibles a las partes interesadas internas y externas relevantes, cuando proceda.

Declan O´Halloran	Aida Durnes	Rafael Hueso	Francisco Domínguez
Managing Director	Chief Operating Officer	Chief Information Officer	Group Head of SHEQ

QuintasGroup
MANAGING POWER

SEVILLE LONDON MIAMI ROME BRISBANE CORK