1. Propósito

El propósito de esta política es definir y establecer un marco de gestión para asegurar la protección y confidencialidad de la información en **Cuarta Esfera,** empresa cuyo alcance es "*Prestación de servicios de topografía e informatización de proyectos, planos y redes de distribución. Realización de proyectos eléctricos en alta y baja tensión. Dirección de obra y Coordinación de Seguridad".*

Esta política está diseñada para cumplir con los requisitos de la norma ISO 27001 y garantizar que la información y los activos relacionados sean protegidos adecuadamente, así como la mejora continua del Sistema de Seguridad de la Información.

---

2. Ámbito de Aplicación

Esta política se aplica a todos los empleados, contratistas, socios y terceros que tengan acceso a los sistemas de información, datos y recursos de **Cuarta Esfera.** Esto incluye, pero no se limita a, los servicios de topografía, informatización de proyectos, y proyectos eléctricos.

---

3. Responsabilidades

- **Consejo de Administración:** Aprobar la política de seguridad de la información y proporcionar los recursos necesarios para su implementación.
- **Responsable de Seguridad de la Información:** Encargado de la implementación, supervisión y mantenimiento de la política de seguridad de la información. Coordina el Sistema de Gestión de Seguridad de la Información (SGSI).
- **Departamento de TI:** Implementar controles técnicos, gestionar el acceso a los sistemas y proporcionar soporte continuo.
- **Usuarios:** Cumplir con esta política y los procedimientos asociados para proteger la información y los recursos de la empresa.

---

4. Objetivos de Seguridad de la Información

- **Confidencialidad:** Proteger la información de accesos no autorizados.
- **Integridad:** Asegurar que la información y los datos sean precisos y completos.
- **Disponibilidad:** Garantizar que la información esté disponible para los usuarios autorizados cuando la necesiten.

---

5. Gestión de Riesgos

- **Identificación de Riesgos:** Realizar evaluaciones de riesgos periódicas para identificar amenazas y vulnerabilidades que puedan afectar la seguridad de la información.
- **Tratamiento de Riesgos:** Implementar controles para mitigar los riesgos identificados. Esto incluye controles técnicos, administrativos y físicos.
- **Revisión de Riesgos:** Revisar y actualizar las evaluaciones de riesgos y las medidas de control de manera regular.

---

6. Control de Acceso

- **Autenticación y Autorización:** Implementar mecanismos de autenticación robustos y asegurar que el acceso a la información y los sistemas se otorgue de acuerdo con el principio de menor privilegio.
- **Gestión de Claves:** Establecer políticas para la creación, uso, y almacenamiento seguro de claves de acceso.

---

7. Protección de la Información

- **Cifrado:** Utilizar cifrado para proteger la información en tránsito y en reposo.
- **Seguridad Física:** Implementar medidas de seguridad física para proteger los equipos y las instalaciones que almacenan o procesan información sensible.
- **Seguridad en la Red:** Aplicar controles de seguridad en la red para proteger contra accesos no autorizados y ataques.

---

8. Formación y Concienciación

- **Capacitación:** Proporcionar formación continua sobre seguridad de la información para todos los empleados y partes interesadas.
- **Concienciación:** Promover una cultura de seguridad mediante campañas de concienciación y comunicación regular sobre la importancia de la seguridad de la información.

---

9. Gestión de Incidentes

- **Reporte de Incidentes:** Establecer procedimientos para el reporte inmediato de incidentes de seguridad de la información.
- **Respuesta a Incidentes:** Desarrollar y mantener un plan de respuesta a incidentes para gestionar y mitigar los efectos de los incidentes de seguridad.

---

10. Cumplimiento, Revisión y Mejora

- **Cumplimiento:** Asegurar el cumplimiento de esta política y de los requisitos legales y reglamentarios aplicables.
- **Auditorías:** Realizar auditorías internas para verificar el cumplimiento de la política y la efectividad de los controles implementados.
- **Revisión de la Política:** Revisar y actualizar esta política al menos anualmente o cuando se produzcan cambios significativos en el entorno de la seguridad de la información.

Campo	Descripción
Nombre del Responsable de Seguridad de la Información	Claudia Benhamou Sáez
Cargo del Responsable	Responsable de Seguridad de la Información
Firma del Responsable	
Fecha de Firma	13/08/2024