Políticas de seguridad

1. Información del proyecto

Nombre del proyecto	Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)
Empresa	Consulting, Knowledge & Systems (CKS)
Fecha de elaboración	25/05/2024
Director del proyecto	Daniel Alexander Gonzales Castillo

2. Introducción

La seguridad de la información es un componente crítico para la operación y la reputación de Consulting, Knowledge & Systems. Este documento establece las políticas de seguridad de la información diseñadas para proteger la confidencialidad, integridad y disponibilidad de los activos de información de la empresa. Estas políticas están alineadas con los estándares internacionales de seguridad, como la ISO/IEC 27001 e ISO/IEC 27005, y tienen como objetivo mitigar los riesgos identificados y priorizados en el análisis de riesgos.

3. Alcance

Estas políticas se aplican a todos los empleados, contratistas y terceros que tienen acceso a los sistemas de información y datos de la empresa. Incluyen tanto los activos físicos como los lógicos y de información, abarcando desde equipos de computación hasta datos sensibles y documentos estratégicos.

4. Objetivos

- Proteger la confidencialidad de la información, asegurando que solo las personas autorizadas tengan acceso.
- Mantener la integridad de la información, previniendo modificaciones no autorizadas.
- Garantizar la disponibilidad de la información, asegurando que esté accesible cuando se necesite.
- Cumplir con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información.

5. Políticas de seguridad

a. Políticas de control de acceso

- **Autenticación y Autorización**: Todos los usuarios deben autenticarse mediante métodos robustos como la autenticación multifactor antes de acceder a los sistemas de información críticos.
- **Control de Accesos**: Se deben definir y aplicar controles de acceso basados en roles (RBAC) para asegurar que los usuarios solo puedan acceder a la información necesaria para sus funciones laborales.

b. Políticas de protección de datos

- **Cifrado de Datos**: La información sensible, como datos de clientes, datos bancarios e informes financieros, debe cifrarse tanto en tránsito como en reposo utilizando algoritmos de cifrado aprobados.
- **Clasificación de Datos**: Todos los datos deben clasificarse en categorías de confidencialidad para determinar los niveles adecuados de protección y control.

c. Políticas de seguridad de la infraestructura

- **Seguridad de Endpoint**: Todos los dispositivos de computación, incluidos los equipos de escritorio y software especializado como AutoCAD, deben tener instalado software de seguridad que incluye antivirus, antimalware y firewalls.
- **Seguridad Física:** Las áreas donde se almacenan activos críticos, como computadoras y documentación técnica, deben tener controles de acceso físico y sistemas de vigilancia en funcionamiento.

d. Políticas de respaldo y recuperación

- Copias de Seguridad: Se deben realizar respaldos periódicos de todos los datos críticos y almacenarlos en ubicaciones seguras y redundantes.
- Planes de Recuperación: Se deben desarrollar y probar regularmente planes de recuperación ante desastres para asegurar la rápida restauración de datos y sistemas críticos.

e. Políticas de gestión de incidentes

- **Plan de Respuesta a Incidentes:** Debe existir un plan de respuesta a incidentes que detalle los procedimientos para identificar, manejar y resolver incidentes de seguridad.
- **Análisis Forense:** Implementar capacidades de análisis forense para investigar incidentes y mejorar las defensas de seguridad existentes.

f. Políticas de capacitación y concientización

- Capacitación Regular: Todos los empleados deben recibir capacitación regular sobre seguridad de la información, incluyendo el reconocimiento de amenazas y las mejores prácticas de seguridad.
- Concienciación Continua: Promover una cultura de seguridad mediante campañas de concienciación continua y actualizaciones regulares sobre nuevas amenazas y políticas de seguridad.

g. Políticas de monitoreo y auditoría

- **Monitoreo Continuo**: Implementar soluciones de monitoreo y detección de intrusiones para identificar y responder a actividades sospechosas en tiempo real.
- **Auditorías de Seguridad:** Realizar auditorías de seguridad periódicas para evaluar la efectividad de los controles de seguridad y asegurar el cumplimiento con las políticas establecidas.

6. Cumplimiento y revisión

El cumplimiento de estas políticas es obligatorio para todos los empleados y partes interesadas. Las políticas de seguridad de la información deben revisarse y actualizarse regularmente para reflejar los cambios en el entorno de amenazas, la tecnología y las regulaciones aplicables.