Plan de gestión de la calidad

1. Información del proyecto

Nombre del proyecto	Plan de mejora 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. Resumen

Este plan de gestión de calidad se ha desarrollado para el proyecto de mejora de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS). El objetivo principal de este plan es establecer un marco de trabajo para garantizar que el proyecto se ejecute de acuerdo con los estándares de calidad establecidos y que los entregables del proyecto cumplan con los requisitos del cliente.

3. Alcance del plan de gestión de calidad

Este plan de gestión de calidad abarca todas las actividades relacionadas con la gestión de la calidad del proyecto, incluyendo:

- **Planificación de la calidad:** Identificación de los estándares de calidad, establecimiento de los objetivos de calidad, definición de las actividades de control de calidad y asignación de roles y responsabilidades.
- **Ejecución de la calidad**: Implementación de las actividades de control de calidad planificadas, monitoreo del desempeño del proyecto en relación con los objetivos de calidad y toma de acciones correctivas cuando sea necesario.
- **Verificación y validación**: Verificación de que los entregables del proyecto cumplen con los estándares de calidad y validación de que el proyecto cumple con los objetivos del cliente.

4. Estándares de calidad

a. ISO/IEC 27001 - Sistema de gestión de la seguridad de la información

La norma ISO/IEC 27001 proporciona un marco integral para la implementación y gestión de un SGSI. Define los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI dentro del contexto de una organización. La adopción de este estándar permitirá:

- **Establecer una política de seguridad de la información:** Define el compromiso de la alta dirección con la seguridad de la información y establece los principios rectores para la gestión de riesgos y la protección de los activos de información.
- **Realizar una evaluación de riesgos**: Identifica los activos de información de la organización, analiza las amenazas y vulnerabilidades, y evalúa los riesgos potenciales para la seguridad de la información.
- **Implementar controles de seguridad**: Establece controles apropiados para mitigar los riesgos identificados, considerando aspectos como el acceso a la información, la confidencialidad, la integridad y la disponibilidad.
- **Medir y monitorear el desempeño:** Establece indicadores de rendimiento y mecanismos de monitoreo para evaluar la efectividad de los controles de seguridad y detectar posibles incidentes.
- **Mejorar continuamente el SGSI:** Implementa un proceso de mejora continua para identificar oportunidades de mejora en el SGSI y adaptarlo a los cambios del entorno.

b. ISO 27005 - Gestión de riesgos de la seguridad de la información en las organizaciones

La norma ISO 27005 complementa a la ISO/IEC 27001 proporcionando directrices para la gestión de riesgos de la seguridad de la información (SGSI). Define un proceso sistemático para identificar, evaluar, tratar y comunicar los riesgos de seguridad de la información en el contexto de una organización. La implementación de ISO 27005 permitirá:

- **Establecer un contexto para la gestión de riesgos**: Define el alcance del SGSI, los objetivos de seguridad de la información y los criterios de riesgo.
- **Identificar los riesgos**: Describe los métodos para identificar y clasificar los riesgos de seguridad de la información, considerando fuentes de riesgo, activos de información y vulnerabilidades.
- **Analizar los riesgos:** Evalúa la probabilidad y el impacto potencial de los riesgos identificados para determinar su prioridad.
- **Evaluar los riesgos:** Prioriza los riesgos de acuerdo con su gravedad y determina las medidas de tratamiento necesarias.
- **Tratar los riesgos:** Implementa las medidas de tratamiento de riesgos seleccionadas, como la eliminación, la reducción, la transferencia o la aceptación del riesgo.

- **Comunicar los riesgos**: Informa a las partes interesadas relevantes sobre los riesgos de seguridad de la información y las medidas de tratamiento implementadas.
- **Monitorear y revisar los riesgos:** Evalúa periódicamente la efectividad de las medidas de tratamiento de riesgos y realiza ajustes según sea necesario.

La implementación conjunta de estos estándares permitirá establecer un enfoque integral para la mejora de la seguridad de la información de la empresa Consulting, Knowledge & Systems (CKS). La ISO/IEC 27001 proporciona el marco general para el SGSI, mientras que la ISO 27005 fortalece la gestión de riesgos dentro del SGSI, asegurando la identificación, evaluación y tratamiento adecuados de los riesgos de seguridad de la información.

5. **Objetivos de calidad**

   Los objetivos de calidad del proyecto son los siguientes:
   - Completar el proyecto dentro del plazo y el presupuesto establecidos.
   - Asegurar que todos los entregables del proyecto cumplan con los requisitos del cliente y los estándares de calidad aplicables.
   - Implementar todos los controles de seguridad de la información planificados.
   - Capacitar al 100% del personal del proyecto en el uso de los nuevos controles de seguridad.
   - Reducir el riesgo de incidentes de seguridad de la información en un 20%.

6. **Roles y responsabilidades**
   - **Gerente de proyecto:** Es responsable de la planificación, ejecución y control de todas las actividades de gestión de la calidad del proyecto.
   - **Equipo del proyecto:** Es responsable de la implementación de las actividades de control de calidad planificadas.
   - **Cliente:** Es responsable de la aprobación de los objetivos de calidad y la aceptación de los entregables del proyecto.

7. **Entregables y procesos del proyecto sujetos a revisión de la calidad**

Entregable	Actividad de calidad
Identificación de activos	
Inventario de activos	Revisión y verificación de la exhaustividad y precisión de los datos recopilados.

Priorización de activos	Análisis detallado de la relevancia y criticidad de los activos identificados.
Evaluación de riesgos y vulnerabilidades	
Informe de identificación de riesgos y vulnerabilidades	Validación de la identificación de riesgos y vulnerabilidades a través de revisiones por pares.
Informe de análisis y priorización de riesgos	Utilización de metodologías estandarizadas para la evaluación de riesgos.
Informe de recomendaciones de mitigación	Validación de las recomendaciones de mitigación con pruebas de concepto o pilotos.
Políticas y procedimientos de seguridad	
Políticas de seguridad	Comparación con las mejores prácticas de la industria y cumplimiento normativo.
Manual de procedimientos de seguridad	Realización de simulaciones para probar la efectividad de los procedimientos.
Implementación de controles de acceso y autenticación	
Informe de controles de acceso	
Informe de pruebas de funcionalidad y seguridad	
Plan de copias de seguridad y recuperación de datos	
Plan de copias de seguridad	Pruebas de respaldo y restauración periódicas para garantizar la efectividad.
Implementación de procedimientos de copias de seguridad	Monitorización continua para detectar y resolver problemas rápidamente.
Informe de pruebas de recuperación de datos	Realización de pruebas de recuperación de datos para evaluar la efectividad.
Capacitación del personal	
Material de capacitación	Revisión y validación del contenido del material por expertos en seguridad.
Sesiones de capacitación programadas y coordinadas	Evaluación de la efectividad de las sesiones mediante encuestas y exámenes.
Formulario de evaluación de la efectividad de	Análisis de las evaluaciones para identificar áreas de mejora.

la capacitación	

8. Actividades de control de calidad y de gestión de calidad previstas en el proyecto

Las siguientes actividades de control de calidad y de gestión de calidad se llevarán a cabo en el proyecto:

- Revisiones de estado del proyecto
- Inspecciones de entregables
- Pruebas de los controles de seguridad
- Encuestas de satisfacción del cliente
- Análisis de causa raíz de incidentes de seguridad
- Auditorías internas de calidad