CASO DE NEGOCIO

Identificador del proyecto: SGP-CKS-01

Versión 1.0

Presentado por:	Ciriaco Esquivel Omar Antonio	**Fecha:**	18/04/2024
Revisado por:	Soto Obregon Milagros Katherine	**Fecha:**	21/04/2024
Aprobado por:	Gonzales Castillo Daniel	**Fecha:**	24/04/2024
Lugar:	Villa el Salvador, Lima, Perú.		

IDENTIFICACIÓN DEL PROYECTO	
1. Nombre del proyecto	Plan de mejora de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)
2. Cliente	Consulting Knowledge & Systems (CKS)
3. Director propuesto	Daniel Gonzales Castillo

CASO DE NEGOCIO

Identificador del proyecto: SGP-CKS-01

Versión 1.0

ALINEAMIENTO DEL PROYECTO	
1. Objetivos estratégicos de la organización	● Consolidación de la posición en el mercado nacional ● Expansión de la cartera de clientes en diferentes industrias ● Liderazgo en la adopción de tecnologías emergentes ● Mejora continua de la capacitación y certificación del personal ● Fortalecimiento de alianzas estratégicas con socios tecnológicos
2. Propósito del proyecto	El proyecto busca fortalecer la protección de datos y sistemas críticos de la empresa, garantizando integridad, confidencialidad y disponibilidad de la información. Se llevarán a cabo acciones como identificación de activos críticos, evaluación de riesgos, implementación de políticas de seguridad y cumplimiento normativo para proteger la infraestructura contra amenazas cibernéticas, asegurando la continuidad del negocio y fortaleciendo la confianza de los clientes.
3. Justificación del proyecto	El proyecto "Plan de mejora de la seguridad de la información para CKS" se justifica por la necesidad de proteger los datos y sistemas críticos de la empresa ante las crecientes amenazas cibernéticas. La iniciativa busca mitigar riesgos, cumplir con regulaciones legales, garantizar la continuidad del negocio y fortalecer la confianza del cliente en CKS.
4. Delimitación del Proyecto:	**Delimitación Espacial:** ● El proyecto se llevará a cabo en las instalaciones de la empresa Consulting Knowledge & Systems (CKS), ubicada en la ciudad de Lima, Perú. ● Las actividades del proyecto se centrarán en las áreas físicas y virtuales de CKS, abarcando sus oficinas, centros de datos y sistemas de información. **Delimitación Temporal:** ● El proyecto comenzará el 17 de abril y se espera que concluya junto a la culminación del presente ciclo. ● El período de ejecución del proyecto se extenderá aproximadamente 12 semanas, durante las cuales se llevarán a cabo todas las actividades planificadas.

CASO DE NEGOCIO

Identificador del proyecto: SGP-CKS-01

Versión 1.0

CONTEXTO DEL PROYECTO

1. Asunciones

a. Los datos necesarios para la implementación del proyecto estarán disponibles en el formato y calidad requeridos.
b. La infraestructura tecnológica existente de la empresa puede soportar las nuevas implementaciones y mejoras sin mayores problemas.
c. Los recursos humanos necesarios estarán disponibles y comprometidos con el proyecto durante su duración.
d. La empresa cuenta con la liquidez para ejecutar el presupuesto establecido.

2. Restricciones

a. No se pueden realizar cambios significativos en los requisitos del proyecto sin la aprobación previa del comité de dirección.
b. No se permitirá la adquisición de recursos adicionales que no estén incluidos en el presupuesto aprobado.
c. No se pueden realizar implementaciones que afecten la disponibilidad de los sistemas críticos durante horas pico de operación sin la debida autorización.
d. No se pueden realizar modificaciones en la infraestructura existente que no estén directamente relacionadas con los objetivos del proyecto.
e. No se permitirá la desviación de los procedimientos de seguridad establecidos sin la aprobación del equipo de seguridad de la información.
f. No se puede comprometer la calidad del trabajo realizado para cumplir con los plazos establecidos.
g. No se permitirá la falta de documentación adecuada y actualizada sobre el progreso y los resultados del proyecto.
h. No se pueden realizar cambios en la programación de las actividades principales del proyecto sin una evaluación exhaustiva de su impacto en el cronograma general.
i. No se pueden realizar compromisos con los proveedores que excedan los términos y condiciones establecidos en los contratos firmados.

3. Riesgos

a. **Interrupción en las Operaciones:** Durante la implementación de nuevas políticas de seguridad, existe el riesgo de interrumpir las operaciones regulares de la empresa, afectando la productividad y la satisfacción del cliente.
b. **Resistencia al Cambio:** El personal podría resistirse a la implementación de nuevas políticas de seguridad, dificultando su adopción efectiva.
c. **Errores en la Configuración:** Existe el riesgo de cometer errores durante la configuración de nuevos controles de seguridad, lo que podría dejar sistemas vulnerables o causar interrupciones en la red.
d. **Falta de Recursos:** La implementación de medidas adicionales podría requerir recursos adicionales, superando las capacidades disponibles y retrasando el proyecto.
e. **Fuga de Información Sensible:** Durante la implementación de controles de acceso, existe el riesgo de brechas de seguridad que permitan el acceso no autorizado a datos sensibles.

CASO DE NEGOCIO

Identificador del proyecto: SGP-CKS-01

Versión 1.0

DESCRIPCIÓN DEL DESARROLLO DE LA PROPUESTA
El desarrollo de la propuesta para fortalecer la seguridad de la información en Consulting Knowledge & Systems (CKS) será un proceso integral que involucra múltiples etapas y actividades diseñadas para cumplir con los objetivos del proyecto. A continuación se detalla cómo se llevará a cabo este proceso: **1. Identificación de Activos de Información Crítica:** **a.** Se realizará una exhaustiva identificación de todos los activos de información crítica de CKS, incluyendo datos, sistemas y recursos de infraestructura de red. **b.** Se clasificarán y priorizarán estos activos según su importancia y valor para la empresa. **2. Evaluación y Mitigación de Riesgos:** **a.** Se llevará a cabo una evaluación detallada de los riesgos asociados con los activos de información identificados, así como de las amenazas y vulnerabilidades potenciales que enfrenta CKS en su entorno operativo. **b.** Se desarrollarán estrategias y medidas para mitigar estos riesgos, priorizando aquellos que representen las mayores amenazas para la integridad, confidencialidad y disponibilidad de los datos críticos de la empresa. **3. Implementación de Políticas y Procedimientos de Seguridad:** **a.** Se diseñarán e implementarán políticas y procedimientos de seguridad de la información que establezcan directrices claras y prácticas para proteger los activos de información de CKS. **b.** Estas políticas y procedimientos abordarán áreas como el control de acceso, la gestión de contraseñas, la protección de datos, la monitorización de eventos y la respuesta a incidentes de seguridad. **4. Cumplimiento de Regulaciones y Normativas:** **a.** Se asegurará el cumplimiento de todas las regulaciones y normativas aplicables en materia de seguridad de la información, garantizando que CKS esté alineado con los estándares de seguridad requeridos por la industria y las autoridades reguladoras. **5. Capacitación del Personal:** **a.** Se proporcionará capacitación y concientización sobre seguridad de la información al personal de CKS, asegurando que estén familiarizados con las políticas y procedimientos de seguridad y puedan contribuir activamente a su implementación y cumplimiento. **6.** Evaluación periódica y monitoreo continuo de la postura de seguridad de la información de CKS, realizando ajustes y mejoras según sea necesario para mantener la protección integral de los datos y sistemas de la empresa. Este proceso de desarrollo de la propuesta se llevará a cabo de manera planificada y coordinada, con la participación activa de los diferentes departamentos y equipos relevantes de CKS. La duración será de 4 meses, comenzando en abril y concluyendo en julio del 2024.

ANÁLISIS DE VIABILIDAD	
1. Viabilidad Técnica:	● La empresa CKS cuenta con experiencia y conocimientos técnicos en el área de tecnologías de la información, lo que proporciona una base sólida para la implementación de medidas de seguridad de la información. ● La disponibilidad de herramientas y tecnologías de seguridad avanzadas en el mercado respalda la viabilidad técnica del proyecto.

2. Viabilidad Financiera:	● Se evaluará y estimará un presupuesto adecuado para el proyecto, lo que permitirá cubrir los costos asociados con la implementación de medidas de seguridad, incluyendo la adquisición de herramientas y tecnologías, la capacitación del personal y los costos operativos. ● La mejora en la seguridad de la información puede traducirse en ahorros a largo plazo al prevenir incidentes de seguridad costosos y mitigar el riesgo de pérdida de datos.
3. Viabilidad Operativa:	● La implementación de políticas y procedimientos de seguridad puede requerir cambios en los procesos operativos de la empresa. Sin embargo, la capacitación adecuada del personal y una comunicación efectiva pueden facilitar la transición hacia un entorno operativo más seguro. ● Es importante garantizar la integración de las medidas de seguridad con las operaciones existentes de la empresa para minimizar cualquier impacto negativo en la productividad y la eficiencia.
4. Viabilidad Legal y Regulatoria:	● La empresa debe asegurarse de cumplir con todas las regulaciones y normativas aplicables en materia de seguridad de la información, lo que puede requerir la implementación de medidas adicionales para garantizar el cumplimiento. ● El cumplimiento de estas regulaciones es fundamental para evitar sanciones legales y proteger la reputación de la empresa.