

	PLAN DE GESTIÓN DE ALCANCE	Versión: <b>2.0-mayo-2024</b>
		Página: <b>1 de 2</b>

**PIAN DE FORTALECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN PARA  
LA EMPRESA CONSULTING, KNOWLEDGE & SYSTEMS (CKS)**

CONTROL DE VERSIONES		
Versión	Hecha Por	Fecha
<b>2.0</b>	<ul style="list-style-type: none"> <li>Soto Obregon Milagros Katherine</li> <li>Gonzales Castillo Daniel Alexander</li> <li>Huánuco Vicuña James Nilton</li> <li>Ciriaco Esquivel Omar</li> <li>Yauricasa Mendoza Miguel Angel</li> <li>Vasquez Leiva Antony</li> </ul>	25/05/2024

NOMBRE DEL PROYECTO
Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)

ALCANCE DEL SERVICIO
Implementar medidas y controles de seguridad de la información para proteger los activos críticos de CKS contra amenazas cibernéticas y físicas.
<p><b>Descripción del Plan de Gestión de Alcance:</b></p> <p>El alcance del proyecto se desarrollará en la siguiente versión del Plan, utilizando la técnica de descomposición, dividiendo el trabajo en componentes más pequeños y manejables. Se realizarán sesiones de planificación con el equipo del proyecto para crear la Estructura de Desglose del Trabajo (EDT) y su Diccionario, que detallarán los entregables específicos, el trabajo requerido y los responsables de cada tarea. Este proceso asegurará que todos los aspectos del proyecto sean considerados y gestionados adecuadamente.</p> <p>La verificación del alcance se realizará mediante inspecciones y revisiones formales con los interesados para asegurarse de que los entregables cumplen con los requisitos establecidos. Se utilizarán documentos como la línea base del alcance y los requisitos del proyecto para guiar estas revisiones.</p>

DESCRIPCIÓN DEL SERVICIO
El servicio garantiza la protección integral de los activos críticos de CKS contra amenazas cibernéticas y físicas mediante la implementación de medidas y controles de seguridad de la información eficaces.

ENTREGABLES DE GESTIÓN
<ul style="list-style-type: none"> <li>Informe de investigación y recopilación de datos</li> <li>Informe de análisis de activos de información</li> </ul>



## PLAN DE GESTIÓN DE ALCANCE

Versión: **2.0-mayo-2024**

Página: **2 de 2**

### ENTREGABLES

- Informe de identificación de riesgos y vulnerabilidades
- Informe de análisis y priorización de riesgos
- Informe de recomendaciones de mitigación
- Políticas de seguridad
- Manual de procedimientos de seguridad documentados
- Informe de controles de acceso
- Informe de pruebas de funcionalidad y seguridad
- Plan de copias de seguridad
- Implementación de procedimientos de copias de seguridad
- Informe de pruebas de recuperación de datos
- Material de capacitación
- Sesiones de capacitación programadas y coordinadas
- Formulario de evaluación de la efectividad de la capacitación

### RESRICCIONES

#### 1. Costo

No se permitirá la adquisición de recursos adicionales que no estén incluidos en el presupuesto aprobado.

#### 2. Tiempo

No se pueden realizar implementaciones que afecten la disponibilidad de los sistemas críticos durante horas pico de operación sin la debida autorización.

#### 3. Calidad

No se puede comprometer la calidad del trabajo realizado para cumplir con los plazos establecidos.

### DICCIONARIO DE LA EDT

Componente	Descripción del trabajo	Responsable
1.1. Identificación de activos de información crítica	Identificar y clasificar los activos de información crítica de la organización.	Ciriaco Esquivel Omar
1.1.1. Informe de investigación y recopilación de datos	Investigar y recopilar datos sobre los activos de información crítica de la organización.	Ciriaco Esquivel Omar
1.1.2. Informe de análisis de activos de información	Analizar los activos de información para identificar su importancia y criticidad.	Ciriaco Esquivel Omar



## PLAN DE GESTIÓN DE ALCANCE

Versión: **2.0-mayo-2024**

Página: **3 de 2**

1.2. Evaluación de riesgos y vulnerabilidades	Realizar evaluaciones de riesgos y vulnerabilidades en los activos de información crítica.	Gonzales Castillo Daniel
1.2.1. Informe de identificación de riesgos y vulnerabilidades	Identificar y documentar los riesgos y vulnerabilidades en los activos de información.	Gonzales Castillo Daniel
1.2.2. Informe de análisis y priorización de riesgos	Analizar y priorizar los riesgos identificados para la toma de decisiones.	Gonzales Castillo Daniel
1.2.3. Informe de recomendaciones de mitigación	Proporcionar recomendaciones para mitigar los riesgos y vulnerabilidades identificados.	Gonzales Castillo Daniel
1.3. Políticas y procedimientos de seguridad	Implementar normativas y estándares de seguridad para garantizar la protección de los activos críticos.	Soto Obregon Milagros
1.3.1. Políticas de seguridad	Desarrollar políticas para establecer las normas y directrices de seguridad de la información.	Soto Obregon Milagros
1.3.2. Manual de procedimientos de seguridad	Documentar los procedimientos operativos estándar para la implementación de las políticas de seguridad.	Soto Obregon Milagros
1.4. Implementación de controles de acceso y autenticación	Establecer y configurar controles de acceso y autenticación para restringir el acceso no autorizado.	Huanuco Vicuña James
1.4.1. Informe de Controles de accesos	Implementar controles de acceso para garantizar la seguridad de los activos de información.	Huanuco Vicuña James
1.4.2. Informe de pruebas de funcionalidad y seguridad	Realizar pruebas para asegurar la funcionalidad y seguridad de los controles de acceso.	Huanuco Vicuña James
1.5. Plan de copias de seguridad y recuperación de datos	Elaborar un plan de copias de seguridad para garantizar la disponibilidad y recuperación de datos críticos.	Yauricasa Mendoza Miguel

	<b>PLAN DE GESTIÓN DE ALCANCE</b>	Versión: <b>2.0-mayo-2024</b>
		Página: <b>4 de 2</b>

1.5.1. Plan de copias de seguridad	Desarrollar un plan para realizar copias de seguridad de los datos críticos de la organización.	Yauricasa Mendoza Miguel
1.5.2. Implementación de procedimientos de copias de seguridad	Implementar procedimientos para llevar a cabo las copias de seguridad de manera efectiva.	Yauricasa Mendoza Miguel
1.5.3. Informe de pruebas de recuperación de datos	Realizar pruebas para garantizar la efectividad de la recuperación de datos en caso de incidentes.	Yauricasa Mendoza Miguel
1.6. Capacitación del personal	Brindar capacitación en seguridad de la información al personal de la organización.	Vasquez Leiva Antony
1.6.1. Material de capacitación	Desarrollar materiales de capacitación para el personal sobre seguridad de la información.	Vasquez Leiva Antony
1.6.2. Sesiones de capacitación programadas y coordinadas	Programar y coordinar sesiones de capacitación para el personal.	Vasquez Leiva Antony
1.6.3. Formulario de evaluación de la efectividad de la capacitación	Evaluar la efectividad de la capacitación mediante formularios de retroalimentación.	Vasquez Leiva Antony

#### 1.1.1. Proceso de Definición del Alcance y Creación de EDT

En el proceso de definición del alcance y creación de la estructura de desglose del trabajo (EDT) para el proyecto de seguridad de la información de CKS, se establecerán los límites y entregables del proyecto. Esto se logrará mediante la descomposición jerárquica de las actividades necesarias para implementar las medidas y controles de seguridad, basada en los entregables y necesidades específicas de CKS.

#### 1.1.2. Proceso de Validación del Alcance

La validación del alcance del proyecto de seguridad de la información de CKS será llevada a cabo por el Scrum Master del proyecto, quien se asegurará de que todos los entregables cumplan con los requisitos definidos y las expectativas de los interesados, incluidos los requisitos del negocio y las necesidades del contrato.

	<b>PLAN DE GESTIÓN DE ALCANCE</b>	Versión: <b>2.0-mayo-2024</b>
		Página: <b>5 de 2</b>

### **1.1.3. Proceso de Control del Alcance**

El control del alcance del proyecto de seguridad de la información de CKS será supervisado por el experto designado para el proyecto. Este experto revisará periódicamente los avances del proyecto y proporcionará orientación sobre cualquier cambio o ajuste necesario para garantizar que el proyecto permanezca dentro de los límites establecidos.