PLAN PARA LA DIRECCIÓN DEL PROYECTO

Título del Proyecto	Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)		
Integrantes:	● Soto Obregon Milagros Katherine ● Gonzales Castillo Daniel Alexander ● Huánuco Vicuña James Nilton ● Ciriaco Esquivel Omar ● Yauricasa Mendoza Miguel Angel ● Vasquez Leiva Antony	**Fecha de Elaboración**	25/05/2024

1. Objetivos del proyecto

Objetivo	Indicador de éxito
Alcance	
Instalar y poner en marcha las medidas y controles de seguridad de la información especificadas en el proyecto.	Todas las medidas y controles de seguridad de la información están implementados y funcionando correctamente en CKS, cumpliendo con los requisitos del proyecto.
Cronograma (Tiempo)	
Establecer un cronograma de actividades detallado	Todas las actividades del proyecto se completaron dentro de los plazos establecidos en el cronograma.
Costo	
Gestionar los costos del proyecto de manera eficiente.	El proyecto se completa dentro del presupuesto asignado y sin exceder los límites establecidos.
Calidad	
Garantizar la implementación de medidas de seguridad de alta calidad.	Las medidas de seguridad implementadas cumplen con los estándares de calidad establecidos y proporcionan una protección efectiva contra posibles amenazas y vulnerabilidades.
Otros	
Identificar y gestionar los riesgos y aspectos adicionales del proyecto.	Los riesgos identificados son gestionados de manera efectiva y se abordan de manera oportuna para garantizar el éxito del proyecto.

2. Gestión de Interesados

La gestión de los interesados es un elemento crucial en el éxito de cualquier proyecto. Para el proyecto de "Plan de fortalecimiento de seguridad de la información para la empresa CKS", es importante identificar y comprender las necesidades, expectativas e intereses de los diferentes grupos de interesados involucrados.

Algunos de los principales interesados en este proyecto incluyen:

- Propietario y gerente general de CKS: como máximo responsable de la empresa, es clave mantenerse informado y alineado con los objetivos y avances del proyecto.
- Departamento de ventas: este equipo debe estar al tanto de las mejoras en

seguridad de la información, ya que pueden impactar en la atención y confianza de los clientes.

- Departamento de recursos humanos: serán responsables de implementar y hacer cumplir las nuevas políticas y procedimientos de seguridad con el personal.
- Departamento de finanzas y contabilidad: deberán gestionar el presupuesto y los costos asociados al proyecto.
- Departamento de proyectos: como equipo encargado de la ejecución, será fundamental su participación activa y colaboración.
- Clientes: la mejora en la seguridad de la información les brindará mayor confianza y satisfacción.
- Proveedores y socios comerciales: deberán alinearse a las nuevas políticas y controles de seguridad implementados.
- Autoridades reguladoras: es importante cumplir con los requisitos y normativas legales aplicables.

Información del contacto:

Interesado	Cargo/Rol	Descripción del Puesto	Contacto	Aptitudes
José Luis Regis Fuentes	Propietario y gerente general de CKS	Líder principal y encargado de la supervisión general de la empresa	ceo@cks.com	Liderazgo, visión estratégica, toma de decisiones
Camilo Leiva	Departamento de ventas	Encargados de promover los productos y servicios de CKS	ventas@cks.com	Negociación, comunicación, orientación al cliente
Rodrigo Alejos	Departamento de recursos humanos	Responsables de la gestión del personal de CKS	rrhh@cks.com	Gestión de talento, comunicación interpersonal, resolución de conflictos
Esteban Sergi	Departamento de finanzas y contabilidad	Encargados de la gestión financiera y contable de CKS	contabilidad@cks.com	Conocimientos financieros, habilidades analíticas, precisión
Juan Valenzuela	Departamento de proyectos	Responsables de la planificación, ejecución y seguimientos de los proyectos realizados por CKS	proyectos@cks.com	Gestión de proyectos, trabajo en equipo, resolución de problemas
_	Clientes	Usuarios finales de los servicios productos de CKS	Correos Propios de los Clientes	Compromiso
-	Proveedores y socios comerciales	Entidades externas que mantienen relaciones comerciales con CKS	Correos Propios de cada proveedor	Comunicación, Compromiso
-	Autoridades reguladoras	Organismos gubernamentales	Correos propios de cada organismo	Responsabilidad, Respeto,

		encargados de regular y supervisar las actividades de CKS		Compromiso

3. Gestión de Alcance

ALCANCE DEL SERVICIO
Implementar medidas y controles de seguridad de la información para proteger los activos críticos de CKS contra amenazas cibernéticas y físicas.

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	
ENTREGABLES	● Informe de investigación y recopilación de datos ● Informe de análisis de activos de información ● 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

DESCRIPCIÓN DE LA GESTIÓN DEL ALCANCE	
1. DEFINIR EL ALCANCE	Se emplearán el Acta de Constitución del Proyecto como datos de entrada. Como herramienta para definir el Alcance, se utilizará las reuniones de equipo donde se ha discutido el tema y organizado la información. Los resultados generados por este

	proceso incluirán el Enunciado del Alcance del Proyecto
2. CREAR ESTRUCTURA DETALLADA(EDT)	El enunciado del alcance se utilizará como dato de entrada, como herramienta, se utilizara la técnica de descomposición a nivel de paquetes, mientras que la salida será la EDT y el diccionario de la EDT.
3. VERIFICAR EL ALCANCE	Se utilizará la Línea Base del Alcance, para la verificación se utilizará la inspección del Estado Completado del Proyecto, mientras que la salida serán los entregables aceptados .
ESTRUCTURA DEL DESGLOSE DEL TRABAJO	
EDT	La estructura del desglose del trabajo (EDT) está planeada usando las etapas del Proyecto como primer nivel de descomposición, empleando la técnica de descomposición a nivel de paquetes de trabajo.

DICCIONARIO DEL 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
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
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

4. Gestión de Cronograma

N	ID	Descripción	Duración (Días)	Comienzo	Fin	Predecesora
1	1.1.1.1	Realizar entrevistas con los responsables de cada área	5	mié 03/04/24	dom 07/04/24	
2	1.1.1.2	Recopilar documentos y registros relevantes sobre los activos de la empresa.	3	mié 03/04/24	vie 05/04/24	
3	1.1.2.1	Analizar la importancia de cada activo de información.	3	lun 08/04/24	mié 10/04/24	1
4	1.1.2.2	Documentar todos los activos de información crítica identificados	4	jue 11/04/24	dom 14/04/24	3
5	1.2.1.1	Realizar un análisis exhaustivo de la infraestructura de TI	4	lun 15/04/24	jue 18/04/24	4
6	1.2.1.2	Identificar puntos débiles en la red a través de herramientas de escaneo de vulnerabilidades	2	vie 19/04/24	sáb 20/04/24	5
7	1.2.2.1	Evaluación de impacto y probabilidad de cada riesgo identificado	3	dom 21/04/24	mar 23/04/24	6
8	1.2.2.2	Priorizar los riesgos según su gravedad y probabilidad de ocurrencia.	2	mié 24/04/24	jue 25/04/24	7
9	1.2.3.1	Desarrollar estrategias y recomendaciones para mitigar los riesgos identificados	3	vie 26/04/24	dom 28/04/24	8
10	1.2.3.2	Priorizar las acciones de mitigación en función de la criticidad de los riesgos	3	vie 26/04/24	dom 28/04/24	8
11	1.3.1.1	Desarrollar políticas de seguridad que aborden el acceso a datos, protección de información y respuesta a incidentes	5	lun 29/04/24	vie 03/05/24	10
12	1.3.1.2	Obtener revisión y aprobación por parte de la gerencia	1	sáb 04/05/24	dom 05/05/24	11
13	1.3.2.1	Crear procedimientos operativos estándar para la implementación de las políticas de seguridad	4	lun 06/05/24	jue 09/05/24	12
14	1.3.2.2	Documentar pasos específicos que deben	3	vie 10/05/24	dom 12/05/24	13

		seguir los empleados				
15	1.4.1.1	Documentar los controles de acceso en los sistemas y aplicaciones	5	lun 13/05/24	lun 22/04/24	14
16	1.4.2.1	Realizar pruebas exhaustivas para verificar la funcionalidad y seguridad de los controles de acceso implementados	5	jue 23/05/24	lun 27/05/24	15
17	1.5.1.1	Diseñar plan detallado que describa cómo se realizarán las copias de seguridad	2	mar 28/05/24	mié 29/05/24	16
18	1.5.2.1	Implementar los procedimientos de copia de seguridad definidos en el plan	3	jue 30/05/24	sáb 01/06/24	17
19	1.5.3.1	Realizar pruebas periódicas para verificar la eficacia del plan de recuperación de datos	1	dom 02/06/24	dom 02/06/24	18
20	1.6.1.1	Desarrollar material de capacitación que aborde las políticas y procedimientos establecidos	3	lun 03/06/24	mié 05/06/24	19
21	1.6.2.1	Programar y coordinar sesiones de capacitación para el personal sobre las mejores prácticas de seguridad de la información	1	jue 06/06/24	jue 06/06/24	20
22	1.6.3.1	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación y la realización de pruebas de conocimientos.	2	vie 07/06/24	sáb 08/06/24	21
		Total Tiempo Invertido en Dias	**67**			

5. Gestión de Costos

PRESUPUESTO DEL PROYECTO

Proyecto: Plan de fortalecimiento de seguridad de la información para la empresa CKS

N	ID	Descripción	Costo (S/.)
1	1.1	Identificación de activos de información crítica	1.466,67
2	1.1.1	Informe de investigación y recopilación de datos	663,34
3	1.1.1.1	Realizar entrevistas con los responsables de cada área	296,67

4	1.1.1.2	Recopilar documentos y registros relevantes sobre los activos de la empresa.	366,67
5	1.1.2	Informe de análisis de activos de información	803,33
6	1.1.2.1	Analizar la importancia de cada activo de información.	450,00
7	1.1.2.2	Documentar todos los activos de información crítica identificados	353,33
8	1.2	Evaluación de riesgos y vulnerabilidades	3.403,34
9	1.2.1	Informe de identificación de riesgos y vulnerabilidades	1.196,67
10	1.2.1.1	Realizar un análisis exhaustivo de la infraestructura de TI	760,00
11	1.2.1.2	Identificar puntos débiles en la red a través de herramientas de escaneo de vulnerabilidades	436,67
12	1.2.2	Informe de análisis y priorización de riesgos	976,67
13	1.2.2.1	Evaluación de impacto y probabilidad de cada riesgo identificado	560,00
14	1.2.2.2	Priorizar los riesgos según su gravedad y probabilidad de ocurrencia.	416,67
15	1.2.3	Informe de recomendaciones de mitigación	1.230,00
16	1.2.3.1	Desarrollar estrategias y recomendaciones para mitigar los riesgos identificados	640,00
17	1.2.3.2	Priorizar las acciones de mitigación en función de la criticidad de los riesgos	590,00
18	1.3	Políticas y procedimientos de seguridad	1.688,33
19	1.3.1	Documento de políticas de seguridad	1.003,33
20	1.3.1.1	Desarrollar políticas de seguridad que aborden el acceso a datos, protección de información y respuesta a incidentes	550,00
21	1.3.1.2	Obtener revisión y aprobación por parte de la gerencia	453,33
22	1.3.2	Procedimientos de seguridad documentados	685,00
23	1.3.2.1	Crear procedimientos operativos estándar para la implementación de las políticas de seguridad	331,67
24	1.3.2.2	Documentar pasos específicos que deben seguir los empleados	353,33
25	1.4	Implementación de controles de acceso y autenticación	1.706,67
26	1.4.1	Configuración de controles de acceso documentada	736,67
27	1.4.1.1	Documentar los controles de acceso en los sistemas y aplicaciones	736,67
28	1.4.2	Informe de pruebas de funcionalidad y seguridad	970,00
29	1.4.2.1	Realizar pruebas exhaustivas para verificar la funcionalidad y seguridad de los controles de acceso implementados	970,00
30	1.5	Plan de copias de seguridad y recuperación de datos	2.236,66
31	1.5.1	Plan de copias de seguridad	718,33
32	1.5.1.1	Diseñar plan detallado que describa cómo se realizarán las copias de seguridad	718,33

33	1.5.2	Implementación de procedimientos de copias de seguridad	695,00
34	1.5.2.1	Implementar los procedimientos de copia de seguridad definidos en el plan	695,00
35	1.5.3	Informe de pruebas de recuperación de datos	823,33
36	1.5.3.1	Realizar pruebas periódicas para verificar la eficacia del plan de recuperación de datos	823,33
37	1.6	Capacitación del personal	2.310,00
38	1.6.1	Material de capacitación	643,33
39	1.6.1.1	Desarrollar material de capacitación que aborde las políticas y procedimientos establecidos	643,33
40	1.6.2	Sesiones de capacitación programadas y coordinadas	670,00
41	1.6.2.1	Programar y coordinar sesiones de capacitación para el personal sobre las mejores prácticas de seguridad de la información	670,00
42	1.6.3	Documento de evaluación de la efectividad de la capacitación	996,67
43	1.6.3.1	Evaluar la efectividad de las sesiones de capacitación mediante la recopilación de retroalimentación y la realización de pruebas de conocimientos.	996,67
	Total		**12.811,67**