Acta de Constitución del Proyecto

Nombre del proyecto: Plan de mejora de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)

Identificador del proyecto: SGP-CKS-01

Fecha elaboración: 18 de abril de 2024

Acta de Constitución del Proyecto

Identificador del proyecto: SGP-CKS-01

Versión 1.0

Contenido

Acta de Constitución del Proyecto

Identificador del proyecto: SGP-CKS-01

Versión 1.0

1. Información del Proyecto

Nombre del proyecto	**Plan de mejora de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)**
Empresa/Organización	**Consulting Knowledge & Systems (CKS)**
Fecha de elaboración	**18 de abril de 2024**
Director del Proyecto	**Daniel Gonzales Castillo**

2. Propósito y Justificación del Proyecto

El propósito de este proyecto es fortalecer la seguridad de la información en la empresa Consulting, Knowledge & Systems (CKS), especializada en switching, redes inalámbricas, videovigilancia IP y cableado estructurado de cobre y enlaces de fibra óptica. El objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de los datos críticos de la empresa, así como proteger su infraestructura de red y sistemas contra posibles amenazas y vulnerabilidades cibernéticas. Mediante la identificación de activos de información crítica, la evaluación y mitigación de riesgos, la implementación de políticas y procedimientos de seguridad, y el cumplimiento de regulaciones y normativas aplicables, este proyecto busca garantizar la protección integral de los datos y sistemas de CKS, asegurando la continuidad del negocio y la confianza de los clientes.

3. Descripción del Proyecto

El proyecto de fortalecimiento de la seguridad de la información en CKS tiene como objetivo principal proteger los activos críticos de la empresa, garantizando la integridad, confidencialidad y disponibilidad de los datos y la infraestructura de red. Para lograr este objetivo, se implementarán una serie de medidas y controles de seguridad, abordando aspectos como la identificación de activos de información crítica, la evaluación y mitigación de riesgos, el desarrollo de políticas y procedimientos de seguridad, y la implementación de controles técnicos y organizativos.

Este proyecto se centra en varios aspectos clave:

- **Identificación de Activos de Información Crítica**: Comenzando por una exhaustiva identificación de los activos de información crítica de la empresa, como datos de clientes, información financiera, propiedad intelectual y otros datos sensibles. Esta fase proporcionará una base sólida para comprender los riesgos potenciales y las áreas prioritarias de protección.

- **Evaluación y Mitigación de Riesgos**: A través de una evaluación detallada de riesgos, se identificarán las posibles amenazas y vulnerabilidades que podrían comprometer la seguridad de los activos de información. Esta evaluación permitirá priorizar los riesgos y desarrollar estrategias efectivas para mitigarlos, minimizando así la exposición a posibles ataques o incidentes de seguridad.

- **Desarrollo de Políticas y Procedimientos de Seguridad**: Se desarrollarán políticas y procedimientos de seguridad de la información claros y específicos para la empresa. Esto incluirá el establecimiento de políticas de manejo de contraseñas, control de acceso a la red, seguridad física de los equipos y protocolos de respuesta a incidentes. Estas políticas proporcionarán un marco sólido para guiar las prácticas de seguridad de la empresa y promover una cultura de seguridad entre los empleados.

- **Implementación de Controles de Acceso y Autenticación**: Se implementarán controles de acceso y autenticación para garantizar que solo usuarios autorizados tengan acceso a los datos y sistemas de la empresa. Esto puede incluir la implementación de autenticación multifactor para una capa adicional de seguridad y la configuración de políticas de acceso basadas en roles para limitar el acceso a la información sensible.

- **Establecimiento de un Plan de Copia de Seguridad y Recuperación de Datos**: Se establecerá un plan integral de copia de seguridad y recuperación de datos para garantizar la disponibilidad y la integridad de la información en caso de fallos del sistema, errores humanos o ataques cibernéticos. Este plan incluirá la programación regular de copias de seguridad y la realización de pruebas de recuperación para garantizar la eficacia del plan.

4. Riesgos principales

- **Interrupción en las Operacione**s: Durante la implementación de nuevas políticas y controles de seguridad, existe el riesgo de interrumpir las operaciones regulares de la empresa, lo que podría afectar la productividad y la satisfacción del cliente.

- **Resistencia al Cambio**: El personal de la empresa podría resistirse al cambio y a la implementación de nuevas políticas y procedimientos de seguridad, lo que podría dificultar la adopción efectiva de las medidas de seguridad propuestas.

- **Errores en la Configuració**n: Durante la configuración de nuevos controles de seguridad, existe el riesgo de cometer errores que podrían dejar sistemas y datos vulnerables o causar interrupciones no planificadas en la red.

- **Falta de recursos**: La implementación de medidas de seguridad adicionales podría requerir recursos adicionales, como tiempo, personal y presupuesto, lo que podría superar las capacidades disponibles y retrasar el progreso del proyecto.

- **Fuga de Información Sensible**: Durante la implementación de controles de acceso y autenticación, existe el riesgo de que se produzcan brechas de seguridad que permitan el acceso no autorizado a datos sensibles de la empresa.

5. Objetivos

a. Objetivo principal

Garantizar la protección integral de los activos críticos de CKS contra posibles amenazas y vulnerabilidades cibernéticas y físicas mediante la implementación de medidas y controles de seguridad de la información efectivo.

b. Objetivos específicos

i. Identificar y documentar todos los activos de información crítica de la empresa Consulting, Knowledge & Systems (CKS).
ii. Realizar una evaluación exhaustiva de riesgos para identificar las posibles amenazas y vulnerabilidades que podrían afectar la seguridad de los activos de información de la empresa.
iii. Desarrollar e implementar políticas y procedimientos de seguridad de la información claros y específicos para CKS, incluyendo el manejo de contraseñas, acceso a la red y respuesta a incidentes.
iv. Implementar controles de acceso y autenticación para garantizar que solo usuarios autorizados tengan acceso a los datos y sistemas de la empresa.

v. Establecer un plan de copia de seguridad y recuperación de datos para garantizar la disponibilidad y la integridad de la información en caso de fallos del sistema o ataques cibernéticos.
vi. Capacitar al personal sobre las mejores prácticas de seguridad de la información, incluyendo cómo reconocer y responder a correos electrónicos fraudulentos y mantener contraseñas seguras.
vii. Mantener actualizados los sistemas y aplicaciones con las últimas actualizaciones y parches de seguridad para mitigar vulnerabilidades conocidas.
viii. Implementar sistemas de monitoreo de seguridad para detectar y responder a posibles intrusiones, malware y otros eventos de seguridad en la red de la empresa.
ix. Asegurar la seguridad física de los equipos de TI y los activos de información mediante el control de acceso a las instalaciones y la protección contra robos, incendios y otros riesgos.
x. Asegurarse de cumplir con las leyes y regulaciones aplicables relacionadas con la protección de datos y la privacidad.

6. Listado de hitos

I. Inicio del Proyecto: Este hito marca el inicio oficial del proyecto, incluyendo la asignación de recursos, la formación del equipo del proyecto y la planificación inicial.
II. Identificación de Activos de Información Crítica: Se completa la identificación y documentación de todos los activos de información crítica de CKS, incluyendo datos de clientes, información financiera y propiedad intelectual.
III. Evaluación de Riesgos y Amenazas: Se realiza una evaluación exhaustiva de riesgos para identificar posibles amenazas y vulnerabilidades que podrían afectar la seguridad de los activos de información de la empresa.
IV. Desarrollo de Políticas y Procedimientos de Seguridad: Se desarrollan políticas y procedimientos de seguridad de la información claros y específicos para CKS, incluyendo el manejo de contraseñas, acceso a la red y respuesta a incidentes.
V. Implementación de Controles de Acceso y Autenticación: Se implementan controles de acceso y autenticación para garantizar que solo usuarios autorizados tengan acceso a los datos y sistemas de la empresa.
VI. Establecimiento del Plan de Copia de Seguridad y Recuperación de Datos: Se establece un plan de copia de seguridad y recuperación de datos para garantizar la disponibilidad y la integridad de la información en caso de fallos del sistema o ataques cibernéticos.
VII. Capacitación del Personal en Seguridad de la Información: Se proporciona capacitación al personal sobre las mejores prácticas de seguridad de la información, incluyendo cómo reconocer y responder a correos electrónicos fraudulentos y mantener contraseñas seguras.
VIII. Implementación de Actualizaciones y Parches de Seguridad: Se implementan actualizaciones y parches de seguridad en los sistemas y aplicaciones para mitigar vulnerabilidades conocidas y proteger contra amenazas conocidas.
IX. Implementación de Sistemas de Monitoreo de Seguridad: Se implementan sistemas de monitoreo de seguridad para detectar y responder a posibles intrusiones, malware y otros eventos de seguridad en la red de la empresa.

X. Auditoría y Revisión Final: Se realiza una auditoría final para evaluar el cumplimiento de los objetivos del proyecto y la efectividad de las medidas de seguridad implementadas.

XI. Cierre del Proyecto: Se completa el proyecto, se entregan los resultados finales y se cierran todas las actividades administrativas y de documentación asociadas.

Cronograma de Hitos del Proyecto

ITEM	ACTIVIDAD	2024															
		ABRIL				MAYO				JUNIO				JULIO			
1	Inicio del proyecto																
2	Identificación de activos de información crítica																
3	Evaluación de Riesgos y Amenazas																
4	Desarrollo de Políticas y Procedimientos de Seguridad																
5	Implementación de Controles de Acceso y Autenticación																
6	Establecimiento del Plan de Copia de Seguridad y Recuperación de Datos																
7	Capacitación del Personal en Seguridad de la Información																
8	Implementación de Actualizaciones y Parches de Seguridad																
9	Implementación de Sistemas de Monitoreo de Seguridad																
10	Auditoría y Revisión Final																
11	Cierre del Proyecto																

7. Lista de Interesados

- Propietario y gerente general de CKS: Dirige y supervisa todas las operaciones de la empresa, estableciendo la visión estratégica y garantizando su implementación.

- Departamento de ventas: Responsable de promover y vender los productos y servicios de CKS para satisfacer las necesidades de los clientes y aumentar los ingresos.

- Departamento de recursos humanos: Gestiona el reclutamiento, capacitación y desarrollo del personal de CKS para mantener un ambiente laboral productivo y satisfactorio.

- Departamento de finanzas y contabilidad: Encargado de gestionar las finanzas y los registros contables de CKS para garantizar una gestión financiera eficiente y cumplir con las obligaciones fiscales.

- Departamento de proyectos:Planifica, ejecuta y supervisa los proyectos de CKS para lograr resultados exitosos y cumplir con los objetivos establecidos.
- Clientes: Usuarios finales de los servicios y productos de CKS.
- Proveedores y socios comerciales: Entidades externas que mantienen relaciones comerciales con CKS.
- Autoridades reguladoras: Organismos gubernamentales encargados de regular y supervisar las actividades de CKS.

8. Criterios de aprobación

- Cumplimiento de Normativas: Verificar que todas las medidas implementadas cumplan con las normativas y regulaciones peruanas aplicables, como la Ley de Protección de Datos Personales y el Reglamento de Seguridad de la Información.
- Cobertura de Activos Críticos: Confirmar que todos los activos de información crítica de CKS, incluyendo datos de clientes, información financiera y propiedad intelectual, estén debidamente protegidos según lo establecido en el proyecto.
- Efectividad de Controles de Seguridad: Evaluar la efectividad de los controles de seguridad implementados, incluyendo controles de acceso, autenticación, monitoreo y detección de amenazas, para garantizar la protección adecuada de los activos de información.
- Capacitación del Personal: Verificar que todo el personal relevante de CKS haya sido adecuadamente capacitado en mejores prácticas de seguridad de la información y esté preparado para reconocer y responder a posibles amenazas.
- Respaldo y Recuperación de Datos: Confirmar que se ha establecido un plan de copia de seguridad y recuperación de datos eficaz para garantizar la disponibilidad y la integridad de la información en caso de fallos del sistema o incidentes de seguridad.
- Actualización y Mantenimiento Continuo: Establecer procedimientos para garantizar que los sistemas y aplicaciones se mantengan actualizados con las últimas actualizaciones y parches de seguridad, y que se realicen evaluaciones periódicas para identificar nuevas amenazas y vulnerabilidades.

- Seguimiento de Incidentes: Establecer un proceso para el seguimiento y la gestión de incidentes de seguridad, incluyendo la documentación adecuada, la investigación de causas raíz y la implementación de medidas correctivas y preventivas.

Responsable de la Aprobación:

El responsable de aprobar y firmar si se cumplen estos criterios es el patrocinador del proyecto, un representante de la alta dirección de CKS. El patrocinador evaluará si se han cumplido los criterios de éxito del proyecto y decidirá si procede su aprobación y cierre.

9. Aprobaciones

_____	_____
Firma del Director del Proyecto	Firma del Patrocinador
_____	_____
Nombre Director del Proyecto	Nombre del Patrocinador