PLAN DE GESTIÓN DE REQUISITOS
VERSIÓN 2.0

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

Identificador del proyecto: SGP-CKS-01

Fecha elaboración: 26 de abril de 2024

1. INFORMACIÓN GENERAL DEL PROYECTO

Nombre del Proyecto	Plan De Fortalecimiento De Seguridad De La Información Para La Empresa Cks
Identificador del Proyecto	SGP-CKS-01
Fecha de Elaboración	26 abril del 2024

2. PROPÓSITO Y JUSTIFICACIÓN DEL PROYECTO

1. Propósito 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.

2. Objetivo Principal

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.

3. ALCANCE DEL PROYECTO

1. 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: Realizar una exhaustiva identificación de los activos de información críticos 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 de Riesgos y Vulnerabilidades: Llevar a cabo una evaluación detallada de riesgos para identificar 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.

- Políticas y Procedimientos de Seguridad: Desarrollar 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: Implementar 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.

- Plan de Copias de Seguridad y Recuperación de Datos: Establecer 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.

- Capacitación del Personal: Implementar un programa de capacitación y sensibilización en seguridad de la información dirigido a todos los empleados de la empresa.

Esto ayudará a crear una cultura de seguridad y asegurará que todo el personal esté familiarizado con las políticas, procedimientos y mejores prácticas de seguridad.

2. Entregables del Proyecto

- Informe de investigacion y recopilacion de datos
- Informe de análisis de activos de información
- Informe de identificación de riesgos y vulnerabilidades
- Informe de analisis y priorizacion de riesgos
- Informe de recomendaciones de mitigación
- Políticas de seguridad
- Manual de Procedimientos de Seguridad
- Informe de controles de accesos
- 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
- Agenda de de sesiones de capacitación
- Formulario de Evaluación de la efectividad de la capacitación

3. Criterios de Éxito del Proyecto

- **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.

4. Identificaciòn de requisitos

a. Requerimientos Funcionales

i. Requisitos de negocio

Requerimiento	Funcionalidad
RF001	Se debe cumplir con las regulaciones y normativas de seguridad de la información.
RF002	Se debe proteger la integridad y confidencialidad de los datos de clientes y empleados.
RF003	Se debe mantener la continuidad del negocio y evitar interrupciones en las operaciones comerciales debido a incidentes de seguridad.
RF004	Se debe proteger la reputación y la confianza del cliente en los servicios proporcionados por la empresa.

ii. Requisitos de los interesados

Requerimiento	Funcionalidad
RF005	Proporcionar una solución de seguridad de la información que sea efectiva y fácil de usar para el personal de la empresa.
RF006	Garantizar que las medidas de seguridad implementadas no interfieran significativamente con las actividades de la empresa.
RF007	Proporcionar capacitación y recursos adecuados para el personal de la empresa sobre las mejores prácticas de seguridad de la información.
RF008	Asegurar la transparencia y la comunicación efectiva sobre el progreso y los resultados del proyecto a todas las partes interesadas.

iii. Requisitos de la Solución

Requerimiento	Funcionalidad
RF009	Implementar controles de acceso y autenticación robustos para proteger los sistemas de cableado estructurado, cámaras de seguridad y switching.
RF010	Establecer políticas y procedimientos de seguridad claros y específicos para la empresa, incluyendo el manejo de contraseñas y la respuesta a incidentes.
RF011	Desarrollar 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 o ataques cibernéticos.
RF012	Implementar sistemas de monitoreo de seguridad para detectar y responder a posibles amenazas.

iv. Requisitos del proyecto

Requerimiento	Funcionalidad
RF013	Establecer un cronograma claro y realista para la implementación de medidas de seguridad de la información.
RF014	Asignar recursos adecuados, incluyendo personal y presupuesto, para la ejecución exitosa del proyecto.
RF015	Definir roles y responsabilidades claros para los miembros del equipo de proyecto y las partes interesadas.
RF016	Realizar pruebas exhaustivas de las soluciones implementadas para garantizar su eficacia y funcionamiento adecuado antes de la implementación completa.

v. Requisitos de la Transición

Requerimiento	Funcionalidad
RF017	Proporcionar capacitación y orientación al personal de la empresa sobre los cambios en las políticas y procedimientos de seguridad de la información.
RF018	Coordinar la transición de manera que minimice las interrupciones en la empresa.
RF019	Establecer un mecanismo para evaluar y monitorear continuamente la efectividad de las medidas de seguridad implementadas y realizar ajustes según sea necesario.
RF020	Asegurar que los activos de información crítica estén debidamente respaldados y protegidos durante el proceso de transición.

b. Requerimientos No Funcionales

i. Requisitos de negocio

Requerimiento	Funcionalidad
RNF001	La solución de seguridad de la información debe cumplir con todas las regulaciones y normas de seguridad aplicables.
RNF002	La solución de seguridad de la información debe garantizar la continuidad del negocio con un tiempo de actividad del 99.9% o superior.
RNF003	La solución de seguridad de la información debe proteger la reputación y la confianza del cliente en los servicios de la empresa.
RNF004	La solución de seguridad de la información debe proteger la reputación y la confianza del cliente en los servicios de la empresa.

ii. Requisitos de los interesados

Requerimiento	Funcionalidad
RNF005	La solución de seguridad de la información debe ser fácil de usar y comprender por el personal de la empresa.
RNF006	La implementación de la solución de seguridad no debe interferir significativamente con las actividades y operaciones de la empresa.
RNF007	La solución de seguridad de la información debe contar con mecanismos de capacitación y soporte efectivos para el personal.
RNF008	La comunicación sobre el proyecto debe ser transparente y efectiva para todas las partes interesadas.

iii. Requisitos de la Solución

Requerimiento	Funcionalidad
RNF009	La solución de seguridad de la información debe tener un diseño modular y flexible que permita la integración con otros sistemas.
RNF010	La solución de seguridad de la información debe ser altamente confiable y disponible con un tiempo de actividad del 99.9% o superior.
RNF011	La solución de seguridad de la información debe tener un alto nivel de rendimiento y eficiencia en el procesamiento de datos.
RNF012	La solución de seguridad de la información debe tener un alto nivel de rendimiento y eficiencia en el procesamiento de datos.

iv. Requisitos del proyecto

Requerimiento	Funcionalidad
RNF013	La solución de seguridad de la información debe ser escalable y adaptable a las necesidades de crecimiento futuras de la empresa.
RNF014	La asignación de recursos, incluyendo personal y presupuesto, debe ser adecuada para la ejecución exitosa del proyecto.
RNF015	Los roles y responsabilidades del equipo de proyecto y partes interesadas deben estar claramente definidos.
RNF016	Las pruebas de la solución de seguridad deben ser exhaustivas y garantizar su eficacia y funcionamiento adecuado.

v. Requisitos de la Transición

Requerimiento	Funcionalidad
RNF017	La transición de la solución de seguridad debe coordinarse de manera que minimice las interrupciones en la empresa.
RNF018	La transición de la solución de seguridad debe coordinarse de manera que minimice las interrupciones en la empresa.
RNF019	La capacitación y orientación al personal sobre los cambios en políticas y procedimientos de seguridad debe ser efectiva.
RNF020	Debe establecerse un mecanismo para evaluar y monitorear continuamente la efectividad de las medidas de seguridad implementadas.