Políticas de seguridad

Nombre del proyecto	**Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)**
Empresa/Organización	**Consulting Knowledge & Systems (CKS)**
Fecha de elaboración	**27 de mayo de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

Las políticas de seguridad de la información de CKS están diseñadas conforme a los estándares internacionales ISO 27001 e ISO 27005, para asegurar la protección de sus activos críticos de información. Estas normas proporcionan un marco sólido para la gestión integral de la seguridad de la información y la evaluación de riesgos, respectivamente.

CKS se compromete a mantener la confidencialidad, integridad y disponibilidad de la información mediante la implementación de controles adecuados. Esto incluye la identificación y evaluación de riesgos de manera sistemática según los principios de la ISO 27005, para mitigar amenazas potenciales que podrían afectar la seguridad de los datos de clientes, proyectos internos y sistemas de información.

Estas políticas no solo cumplen con los estándares regulatorios aplicables, sino que también establecen directrices claras para todos los empleados, contratistas y terceros que interactúen con los recursos de información de CKS. Promueven una cultura organizacional de seguridad informática, donde cada miembro del equipo comprende su rol en la protección de los activos de información y está capacitado para responder adecuadamente a incidentes de seguridad.

Al adherirse a estos estándares reconocidos a nivel internacional, CKS no solo mejora su postura de seguridad, sino que también fortalece la confianza de sus clientes y socios comerciales en la gestión responsable de la información confidencial y crítica para el negocio.

2. Objetivos

- **Salvaguardar la información confidencial y crítica de la empresa y sus clientes**
  Este objetivo se centra en proteger la información sensible y crítica de CKS, así como la información confidencial de sus clientes. Esto incluye datos financieros, estrategias de negocio, propiedad intelectual y cualquier otra información que sea vital para el funcionamiento y la reputación de la empresa. Salvaguardar esta información implica implementar controles adecuados de acceso, cifrado, almacenamiento seguro y políticas claras de manejo de datos.
- **Minimizar el riesgo de acceso no autorizado, pérdida o robo de información:**
  Este objetivo busca reducir al mínimo la probabilidad de que la información sensible sea accedida, alterada o eliminada por personas no autorizadas. Se logra mediante la implementación de controles de acceso estrictos, como autenticación multifactor y políticas de gestión de contraseñas robustas. Además, implica la vigilancia continua de los sistemas de seguridad, la detección proactiva de amenazas y la respuesta rápida a incidentes de seguridad.

- **Cumplir con los requisitos legales y contractuales relacionados con la seguridad de la información:**
  CKS se compromete a cumplir con todas las leyes, regulaciones y normativas aplicables en relación con la seguridad de la información. Esto incluye leyes de protección de datos, normas industriales específicas y cualquier requisito contractual establecido por clientes o socios comerciales. Cumplir con estos requisitos no solo asegura la conformidad legal, sino que también fortalece las relaciones comerciales y la confianza del cliente.
- **Promover la conciencia y la responsabilidad en materia de seguridad informática entre todos los empleados y colaboradores:**
  Este objetivo se centra en educar y sensibilizar a todos los miembros del equipo sobre las mejores prácticas de seguridad informática. Esto incluye la realización de programas de formación periódicos, simulacros de phishing, sesiones informativas y la distribución de políticas y procedimientos de seguridad. Fomentar una cultura de seguridad informática asegura que cada individuo comprenda su papel en la protección de los activos de información de CKS y esté preparado para identificar y reportar posibles amenazas.

3. Alcance

El alcance de las políticas de seguridad de la información para CKS abarca todos los activos críticos de información de la empresa, garantizando una protección integral y consistente en diversos niveles y áreas funcionales. Aquí se detalla más sobre el alcance:

Alcance de las Políticas de Seguridad de la Información para CKS:
Estas políticas se aplican a:

- **Sistemas Informáticos**: Incluyendo servidores, estaciones de trabajo, dispositivos móviles y cualquier otro dispositivo utilizado para procesar, almacenar o transmitir información crítica de CKS.
- **Redes**: Todos los componentes de red, incluyendo hardware (routers, switches, firewalls) y software (protocolos, configuraciones de seguridad), que facilitan la conectividad y comunicación dentro y fuera de la organización.
- **Datos Electrónicos:** Todos los datos digitales y electrónicos almacenados en sistemas informáticos, bases de datos, aplicaciones empresariales y cualquier otro medio electrónico utilizado por CKS para la gestión de información.
- **Documentación Física**: Documentos impresos, archivos físicos y cualquier otra forma de registro físico que contenga información sensible o crítica de la empresa.

Estas políticas no están limitadas a un departamento específico o a ciertos niveles jerárquicos; se extienden a todos los niveles de la organización y a todas las áreas funcionales que manejan información sensible o crítica. Esto incluye, pero no se limita a, departamentos como desarrollo de proyectos, recursos humanos, administración financiera, soporte técnico y atención al cliente. El objetivo es asegurar que todas las operaciones y procesos dentro de CKS cumplan con los estándares de seguridad establecidos, minimizando los riesgos de exposición, pérdida o mal uso de la información sensible. Al establecer un alcance amplio y claro, CKS garantiza una protección coherente y efectiva de sus activos de información en toda la organización.

4. Políticas de seguridad

a. Definir los procedimientos para gestionar y controlar tanto el acceso físico como lógico a los sistemas y datos de la empresa, incluyendo la implementación de autenticación multifactor (MFA) en sistemas críticos y la aplicación del principio de privilegios mínimos para asignar y revocar derechos de acceso.

b. Establecer requisitos claros para la creación y gestión de contraseñas seguras, incluyendo la rotación periódica de contraseñas y el uso de cifrado para almacenamiento seguro. Promueve el uso de autenticación de contraseña robusta para proteger los sistemas contra accesos no autorizados.

c. Definir normas para configurar de manera segura los equipos de red, como firewalls, routers y switches. Incluye monitoreo y auditoría regular de la actividad de red para detectar intrusiones y establecer procedimientos para la gestión de vulnerabilidades y aplicaciones de parches de seguridad.

d. Establecer un proceso formal para la notificación, gestión y resolución de incidentes de seguridad. Define roles y responsabilidades claros dentro del equipo de respuesta a incidentes y promueve la realización de simulacros periódicos para mejorar la preparación del personal frente a amenazas.

e. Definir las condiciones bajo las cuales los empleados pueden utilizar los recursos informáticos de la empresa, especificando actividades prohibidas como el acceso no autorizado a sistemas o la divulgación no autorizada de información confidencial.

f. Establecer procedimientos para realizar copias de seguridad regulares de datos críticos y sistemas, asegurando su almacenamiento seguro y protegido contra alteraciones. Incluye pruebas periódicas de recuperación de datos para garantizar la disponibilidad y la integridad de la información en caso de pérdida.

g. Implementar programas regulares de formación y concienciación en seguridad para todos los empleados, educándolos sobre las amenazas actuales, prácticas seguras en el uso de la tecnología y políticas internas de seguridad. Fomenta una cultura organizacional de responsabilidad compartida en la protección de los activos de información de la empresa.