Manual de procedimientos 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

El manual de procedimientos de seguridad de CKS proporciona un marco detallado y estructurado para la implementación efectiva de políticas clave de seguridad de la información. Estas políticas abarcan desde el control de acceso físico y lógico mediante la gestión rigurosa de derechos y la implementación de autenticación multifactor, hasta la gestión proactiva de contraseñas seguras y el cifrado robusto de datos almacenados. Además, se establecen directrices claras para asegurar la configuración segura de redes y la monitorización continua para detectar y mitigar amenazas. El manual también detalla la respuesta a incidentes con un proceso formal y simulacros periódicos, y establece normativas para el uso adecuado de recursos informáticos, la realización de copias de seguridad regulares con almacenamiento seguro y pruebas de recuperación de datos. Finalmente, se enfatiza la importancia de programas educativos en seguridad y la promoción de una cultura organizacional de responsabilidad compartida en la protección de activos de información crítica para la empresa.

2. Objetivos

a. **Gestionar y controlar el acceso seguro**: Implementar procedimientos para gestionar tanto el acceso físico como lógico a los sistemas y datos de CKS, asegurando la protección adecuada mediante la autenticación multifactor y la gestión rigurosa de privilegios mínimos.
b. **Garantizar contraseñas seguras**: Establecer requisitos claros y procedimientos para la creación, gestión y almacenamiento seguro de contraseñas, incluyendo la rotación periódica y el cifrado de contraseñas almacenadas.
c. **Asegurar la integridad de la red:** Definir normativas para configurar y mantener de forma segura los equipos de red, como firewalls, routers y switches, junto con monitoreo y auditoría regular para detectar y responder a intrusiones o actividades maliciosas.
d. **Responder efectivamente a incidentes de seguridad**: Establecer un proceso formal para la notificación, gestión y resolución de incidentes de seguridad, con roles y responsabilidades claros y simulacros periódicos para mejorar la preparación del personal.
e. **Promover el uso adecuado de los recursos de información**: Definir políticas claras sobre el uso aceptable de los recursos informáticos de CKS, prohibiendo actividades no autorizadas y garantizando la confidencialidad de la información sensible.
f. **Asegurar la disponibilidad y recuperación de datos**: Establecer procedimientos para realizar copias de seguridad regulares de datos críticos, almacenarlas de manera segura y probar la recuperación de datos para garantizar su disponibilidad en caso de incidentes o desastres.

g. **Educación y concienciación en seguridad**: Implementar programas regulares de formación y concienciación en seguridad para todos los empleados, promoviendo prácticas seguras y una cultura organizacional de responsabilidad compartida en la protección de activos de información de la empresa.

3. Alcance

El alcance del manual de procedimientos de seguridad de CKS abarca todos los aspectos relacionados con la gestión y protección de la información dentro de la empresa. Esto incluye la administración de accesos físicos y lógicos a los sistemas y datos, la gestión de contraseñas seguras, la configuración y monitoreo de la seguridad de redes, la respuesta a incidentes de seguridad, el uso aceptable de recursos de información, la planificación y ejecución de copias de seguridad y la educación continua en prácticas de seguridad para todos los empleados. Este manual se aplica a todos los departamentos de CKS y a todos los niveles de la organización para asegurar una implementación consistente y efectiva de las políticas de seguridad.

4. Directrices de seguridad

a. Política de Control de Acceso:

i. Gestión y Control de Acceso Físico y Lógico:
Establecer procedimientos para la gestión y control del acceso físico y lógico a los sistemas y datos de CKS. Incluir la identificación de usuarios autorizados, la asignación de credenciales adecuadas, y la revisión y actualización periódica de permisos de acceso.

ii. Implementación de Autenticación Multifactor (MFA):
Definir el procedimiento para implementar la autenticación multifactor en todos los sistemas críticos de CKS. Esto incluye la configuración y administración de MFA para garantizar que cada acceso esté protegido por múltiples capas de verificación.

iii. Asignación y Revocación de Derechos de Acceso:
Detallar el proceso para la asignación y revocación de derechos de acceso, basado en el principio de privilegios mínimos para reducir riesgos de acceso no autorizado.

b. Política de Gestión de Contraseñas:

i. Creación y Gestión de Contraseñas Seguras:
Establecer requisitos claros para la creación y gestión de contraseñas seguras, incluyendo longitud mínima, complejidad y frecuencia de cambio.

ii. Rotación Periódica de Contraseñas:
Definir el procedimiento para la rotación periódica de contraseñas y la prohibición del uso de contraseñas compartidas o débiles.

iii. Cifrado de Contraseñas y Autenticación Robusta:
Detallar cómo se implementará el cifrado de contraseñas almacenadas y asegurar la autenticación robusta en todos los sistemas y aplicaciones críticas.

c. Política de Seguridad de Redes:

i. Configuración Segura de Equipos de Red:
Definir normas para la configuración segura de firewalls, routers y switches, asegurando que todos los dispositivos estén correctamente configurados para mitigar riesgos.

ii. **Monitoreo y Auditoría de Actividad de Red:**
Establecer procedimientos para el monitoreo y la auditoría regular de la actividad de red, con el fin de detectar intrusiones y actividades maliciosas de manera proactiva.

iii. **Gestión de Vulnerabilidades y Parches de Seguridad:**
Detallar cómo se gestionarán las vulnerabilidades y la aplicación de parches de seguridad en los equipos de red, garantizando que todos los dispositivos estén actualizados y protegidos.

d. **Política de Gestión de Incidentes:**

i. **Proceso Formal para la Gestión de Incidentes:**
Describir el proceso formal para la notificación, gestión y resolución de incidentes de seguridad, incluyendo la asignación de roles y responsabilidades dentro del equipo de respuesta a incidentes.

ii. **Simulacros Periódicos de Incidentes:**
Establecer el procedimiento para realizar simulacros periódicos de incidentes, con el objetivo de evaluar la efectividad del plan de respuesta y mejorar la preparación del personal ante posibles emergencias.

e. **Política de Uso Aceptable de Recursos de Información:**

i. **Condiciones de Uso de Recursos Informáticos:**
Definir las condiciones bajo las cuales los empleados pueden utilizar los recursos informáticos de la empresa, especificando las actividades permitidas y prohibidas para proteger la seguridad de la información.

f. **Política de Copias de Seguridad y Recuperación de Datos:**

i. **Procedimientos para Realizar Copias de Seguridad:**
Establecer procedimientos detallados para realizar copias de seguridad regulares de datos críticos y sistemas, asegurando la disponibilidad continua y protegiendo la integridad de la información.

ii. **Almacenamiento Seguro de Copias de Seguridad:**
Describir cómo se almacenarán las copias de seguridad de manera segura, fuera del sitio y en un formato protegido contra alteraciones, para garantizar su disponibilidad en caso de pérdida de datos.

iii. **Pruebas Regulares de Recuperación de Datos:**
Detallar el procedimiento para realizar pruebas regulares de recuperación de datos, asegurando que las copias de seguridad sean efectivas y la información esté disponible en caso de incidente.

g. **Política de Educación y Concienciación en Seguridad:**

i. **Programas de Formación en Seguridad:**
Implementar programas regulares de formación y concienciación en seguridad para todos los empleados, educándolos sobre las amenazas actuales, prácticas seguras y políticas internas de seguridad.

ii. **Cultura de Responsabilidad en la Protección de Activos de Información:**
Fomentar una cultura organizacional de responsabilidad compartida en la protección de los activos de información de CKS, promoviendo la participación activa y el compromiso de todos los empleados.