Implementación de procedimientos de copias 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

Se establece un marco detallado para asegurar la disponibilidad continua y proteger la integridad de la información crítica de la empresa. Inicia con una introducción sobre la importancia estratégica de las copias de seguridad y enumera objetivos claros centrados en la protección de datos. El alcance del documento cubre los sistemas y datos específicos de la empresa, delineando responsabilidades departamentales y procedimientos detallados. Los procedimientos incluyen planificación de copias, ejecución, almacenamiento seguro y pruebas de recuperación de datos, garantizando que cada paso sea ejecutado de manera efectiva y segura. Además, se designan responsabilidades específicas y se establece un plan de mantenimiento continuo para asegurar la eficacia a largo plazo del plan de copias de seguridad de CKS.

2. Objetivos

a. **Asegurar la Disponibilidad Continua**: Garantizar que los datos críticos de la empresa estén disponibles en todo momento mediante la implementación de procedimientos robustos de copia de seguridad y recuperación.
b. **Proteger la Integridad de la Información:** Mantener la integridad de los datos asegurando que las copias de seguridad estén almacenadas de manera segura y protegidas contra modificaciones no autorizadas.
c. **Cumplir con los Requisitos Regulatorios y de Negocio:** Asegurar que las prácticas de copia de seguridad cumplan con las normativas legales y los requisitos internos de la empresa, minimizando el riesgo de pérdida de datos y asegurando la continuidad del negocio.
d. **Minimizar el Tiempo de Inactividad:** Reducir al mínimo el tiempo de inactividad en caso de pérdida de datos mediante la ejecución efectiva de planes de recuperación respaldados por pruebas periódicas de recuperación de datos.
e. **Capacitar al Personal y Mejorar la Conciencia de Seguridad:** Educar a los empleados sobre la importancia de las copias de seguridad y proporcionar capacitación continua para mejorar la conciencia y la responsabilidad en la protección de los activos de información de la empresa.

3. Alcance

a. **Todos los Datos Críticos y Sistemas Informáticos**: Se cubrirán todas las bases de datos, aplicaciones empresariales, archivos críticos y sistemas informáticos utilizados por CKS para sus operaciones diarias.

b. **Todos los Departamentos y Empleados:** Los procedimientos se aplicarán a todos los empleados y departamentos de CKS, asegurando una protección uniforme y consistente de la información en toda la organización.
c. **Almacenamiento y Gestión de Copias de Seguridad:** Incluye la definición de procedimientos para realizar, almacenar y gestionar copias de seguridad de manera segura, fuera del sitio y en un formato que garantice la integridad de los datos.
d. **Pruebas y Validación:** Establecerá la metodología para realizar pruebas regulares de recuperación de datos para asegurar la eficacia de los procedimientos de copia de seguridad y la capacidad de respuesta ante posibles incidentes.
e. **Cumplimiento Normativo:** Asegurará que los procedimientos cumplan con los requisitos legales y normativos aplicables relacionados con la protección de datos y la continuidad del negocio.
f. **Capacitación y Concienciación**: Incluirá la capacitación continua de los empleados sobre las mejores prácticas de seguridad en copias de seguridad, promoviendo una cultura organizacional de protección de activos de información.

4. Procedimientos para realizar las copias 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.