Plan 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	**01 de junio de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

El plan de copias de seguridad de CKS se fundamenta en la necesidad de garantizar que la información crítica de la empresa esté siempre disponible y protegida contra diversos riesgos que podrían comprometer su integridad o disponibilidad. Este plan se concibe como una parte integral de la estrategia de seguridad de la información de CKS, destinado a mitigar las posibles consecuencias de pérdida de datos y a asegurar una pronta recuperación ante incidentes que puedan afectar la operatividad normal de la organización.

2. Objetivos

a. Asegurar la Disponibilidad Continua de Datos Críticos:

- Las copias de seguridad regulares garantizan que la información vital para las operaciones diarias de CKS esté siempre accesible, incluso en situaciones de emergencia como fallos de hardware, errores humanos o ciberataques.
- La disponibilidad continua de datos minimiza el tiempo de inactividad y asegura la continuidad del negocio, permitiendo a CKS mantener operativas sus funciones esenciales sin interrupciones significativas.

b. Proteger la Integridad de la Información:

- Mediante la implementación de procedimientos rigurosos de respaldo y almacenamiento seguro, se evita la alteración, destrucción o pérdida accidental de datos críticos.
- La protección de la integridad de la información asegura que CKS pueda mantener la confianza de sus clientes y socios comerciales al salvaguardar la precisión y fiabilidad de los datos manejados.

3. Alcance

El alcance del plan incluye todos los sistemas informáticos, redes y datos electrónicos utilizados por CKS, abarcando desde servidores y estaciones de trabajo hasta bases de datos y aplicaciones críticas. Se centra en establecer prácticas consistentes y eficientes para la gestión

de copias de seguridad, asegurando que todos los activos de información relevantes estén protegidos de manera adecuada y puedan ser restaurados rápidamente en caso de necesidad.

Este enfoque proactivo no solo reduce la exposición a riesgos operativos, sino que también refuerza la capacidad de CKS para mantener la continuidad del negocio y cumplir con las expectativas de sus partes interesadas en términos de seguridad y confiabilidad de la información.

4. Procedimientos de copias de seguridad

a. Programación y Automatización de Copias de Seguridad

i. **Descripción**: Las copias de seguridad se programarán y automatizarán para garantizar la regularidad y consistencia en la protección de datos.

ii. **Acción a Seguir:**

- **Programación Regular**: Utilización de software especializado para establecer horarios automáticos de copias de seguridad diarias, semanales y mensuales, dependiendo de la criticidad de los datos.
- **Configuración de Retención:** Establecimiento de políticas de retención para determinar la duración durante la cual se conservarán las copias de seguridad antes de su eliminación o reemplazo.

iii. **Responsable:** El responsable de IT o el equipo técnico designado será responsable de configurar y mantener la programación automatizada de las copias de seguridad.

b. Métodos de Almacenamiento y Retención

i. **Descripción**: Los métodos de almacenamiento y retención asegurarán que los datos estén disponibles para restauración cuando sea necesario, manteniendo una política de retención adecuada.

ii. **Acción a Seguir**:

- **Almacenamiento Redundante**: Utilización de múltiples medios de almacenamiento como unidades de disco externas y servicios de almacenamiento en la nube para garantizar la accesibilidad y la redundancia de los datos.
- **Política de Retención:** Establecimiento de períodos de retención específicos basados en la criticidad de los datos y los requisitos regulatorios.

iii. **Responsable:** El equipo de IT será responsable de seleccionar y administrar los métodos de almacenamiento adecuados, asegurando que las políticas de retención se implementen correctamente.

c. Monitoreo y Pruebas de Recuperación

i. **Descripción:** Se establecerá un proceso para monitorear la efectividad de las copias de seguridad y realizar pruebas de recuperación periódicas para verificar la integridad de los datos.

ii. Acción a Seguir:

- **Monitoreo Continuo**: Implementación de herramientas de monitoreo para supervisar el estado de las copias de seguridad y recibir alertas sobre posibles fallos o problemas.
- **Pruebas de Recuperación**: Programación regular de pruebas de restauración para verificar la integridad de los datos y la eficacia del proceso de recuperación en caso de pérdida.
- **Responsable:** El equipo técnico será responsable de realizar pruebas de recuperación periódicas y mantener registros detallados de las actividades de monitoreo.

d. Seguridad de las Copias de Seguridad

i. **Descripción:** Se implementarán medidas de seguridad para proteger las copias de seguridad contra accesos no autorizados y asegurar su integridad.

ii. Acción a Seguir:

- **Cifrado de Datos**: Aplicación de cifrado robusto tanto durante la transmisión como en el almacenamiento de las copias de seguridad para proteger la confidencialidad de la información.
- **Control de Acceso**: Implementación de controles de acceso estrictos para limitar la disponibilidad de las copias de seguridad solo a personal autorizado.
- **Ubicación Segura:** Almacenamiento físico seguro de los medios de copia de seguridad en instalaciones protegidas contra el acceso no autorizado y condiciones ambientales adversas.

iii. **Responsable**: El responsable de seguridad de IT será responsable de implementar y mantener las medidas de seguridad para las copias de seguridad, asegurando que se cumplan las políticas de acceso y cifrado.