Protocolos para la recuperación de información y datos

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	**26 de mayo de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

Este documento comprende los protocolos para la recuperación de información y datos en Consulting, Knowledge & Systems (CKS). Se centra en establecer procedimientos claros y estructurados para garantizar la disponibilidad, integridad y rápida recuperación de datos críticos en caso de incidentes. Inicia con la evaluación de impacto y priorización de incidentes, seguido por la activación inmediata de un equipo de respuesta dedicado a la mitigación del problema y la recuperación de datos. Se detallan procedimientos para la restauración desde copias de seguridad y la validación exhaustiva de los datos recuperados antes de su implementación. Además, se incluyen medidas para la documentación detallada de cada paso del proceso, análisis post-recuperación y la capacitación continua del personal para mejorar la preparación y respuesta ante futuros incidentes.

2. Objetivos

Se definen los siguientes objetivos:

- **Garantizar la disponibilidad de datos críticos**: Se establecerán procedimientos robustos para asegurar que los datos esenciales para sus operaciones estén disponibles en todo momento. Esto incluye la implementación de sistemas de respaldo y redundancia que permitan la rápida recuperación de datos en caso de fallas o pérdidas.
- **Minimizar el tiempo de inactividad:** Se establecerán procedimientos detallados y escalonados para reducir al mínimo el tiempo de inactividad en situaciones de pérdida de datos. Esto implica la configuración de planes de respuesta rápida y la capacitación del personal en la ejecución efectiva de estos planes para mitigar impactos operativos adversos.
- **Proteger la integridad de los datos**: CKS pondrá en práctica medidas rigurosas para asegurar la integridad y precisión de los datos recuperados durante los procesos de recuperación. Esto incluirá la validación continua de datos durante las fases de

restauración y la implementación de controles de seguridad adecuados para prevenir la manipulación o corrupción de datos durante y después del proceso de recuperación.

- **Cumplir con normativas y estándares:** Los protocolos de recuperación de datos de CKS estarán alineados con las normativas y estándares de seguridad pertinentes, como la ISO 27001. Esto asegurará que todos los procesos de recuperación cumplan con las mejores prácticas reconocidas a nivel internacional, garantizando la protección de la información sensible y el cumplimiento de las obligaciones legales y regulatorias.

3. Procedimientos de recuperación de información y datos

a. Evaluación de impacto y priorización

i. Identificación de incidentes

Es fundamental establecer un proceso estructurado y proactivo para identificar y categorizar incidentes que puedan requerir la recuperación de datos en CKS. Esto implica:

- **Monitoreo continuo:** Implementar sistemas de monitoreo continuo de seguridad y operaciones para detectar anomalías y eventos que puedan indicar una posible pérdida de datos.
- **Reporte de incidentes:** Establecer canales claros y procedimientos definidos para que los empleados reporten cualquier incidente o irregularidad que afecte la disponibilidad o integridad de los datos.
- **Clasificación de incidentes:** Categorizar los incidentes según su gravedad y impacto potencial en las operaciones y la continuidad del negocio. Esto permite priorizar adecuadamente las acciones de respuesta y recuperación.

ii. Análisis de impacto

El análisis de impacto es crucial para evaluar las repercusiones potenciales de la pérdida de datos en CKS y orientar las decisiones de recuperación. Incluye:

- **Evaluación de consecuencias**: Determinar las consecuencias operativas y financieras de la pérdida de datos, considerando aspectos como la interrupción de servicios, pérdida de clientes, daños a la reputación y posibles implicaciones legales.
- **Identificación de activos críticos:** Identificar los activos de información críticos para las operaciones de CKS y evaluar su valor estratégico y sensibilidad. Esto ayuda a priorizar la recuperación de datos según la importancia y el impacto en el negocio.
- **Análisis de vulnerabilidades**: Analizar las vulnerabilidades que contribuyen a la ocurrencia de incidentes de pérdida de datos, como

brechas de seguridad, errores humanos o fallos tecnológicos, para implementar medidas preventivas y correctivas efectivas.

b. Respuesta inmediata

i. Activación del equipo de respuestas

Se deberá establecer un protocolo claro para movilizar un equipo dedicado ante la identificación de un incidente que requiera recuperación de datos. Este equipo estará compuesto por personal capacitado en gestión de incidentes y recuperación de datos, quienes estarán disponibles de manera inmediata para iniciar las acciones necesarias según el plan predefinido.

ii. Aislamiento de incidentes

Como parte de la respuesta inicial, se deberá implementar procedimientos para aislar las causas raíz del incidente tan pronto como sea posible. Esto se llevará a cabo con el objetivo de prevenir una mayor pérdida de datos y mitigar futuros riesgos para la seguridad de la información. El proceso incluirá la identificación y desconexión de las fuentes o sistemas afectados, asegurando que el incidente no se propague ni comprometa otros activos críticos de la organización.

c. Recuperación de datos

i. Planificación de recuperación

Se propone desarrollar planes detallados de recuperación que contemplen procedimientos específicos para restaurar datos desde copias de seguridad o medios alternativos en caso de incidentes. Esto debe incluir la identificación de las fuentes de datos críticos y la documentación de los procedimientos necesarios para restaurar estos datos de manera efectiva y eficiente. Se deberán establecer criterios claros para la priorización de la recuperación según la criticidad de la información y los impactos operativos.

ii. Validación de datos

Se implementará un proceso riguroso para verificar la integridad y precisión de los datos recuperados antes de su restauración completa en los sistemas operativos. Esto incluirá pruebas y verificaciones detalladas para asegurar que los datos recuperados sean exactos y estén libres de corrupción o alteración. La validación se realizará utilizando métodos como comparaciones con las versiones anteriores de los datos, verificación cruzada con registros de auditoría, y pruebas de funcionalidad para asegurar que los datos restaurados cumplan con los estándares de calidad y precisión requeridos por CKS y las normativas aplicables.

d. Restauración de sistemas

i. Restablecimiento de sistemas

El proceso de restablecimiento de sistemas se llevará a cabo de la siguiente manera.

- **Utilización de copias de seguridad:** Se restaurarán los sistemas afectados utilizando las copias de seguridad disponibles. CKS mantendrá copias de seguridad actualizadas y accesibles para minimizar el tiempo de inactividad en caso de incidentes.
- **Garantía de funcionamiento normal:** Se verificará que los sistemas restaurados funcionen de acuerdo con las especificaciones operativas normales de la empresa. Esto implica asegurar que todas las aplicaciones y servicios críticos estén completamente operativos y que la conectividad de red sea estable y segura.

ii. **Pruebas de funcionalidad**

Se deberán hacer pruebas exhaustivas para asegurar la funcionalidad y seguridad de los sistemas restaurados

- **Escenarios de prueba complejos:** Se ejecutarán escenarios de prueba que cubran todas las funcionalidades críticas de los sistemas restaurados. Esto incluirá pruebas de integridad de datos, verificación de accesos y permisos, y pruebas de resistencia para evaluar el rendimiento bajo carga.
- **Validación de requisitos operativos y de seguridad:** Las pruebas se realizarán para garantizar que los sistemas restaurados cumplan con los requisitos operativos y de seguridad establecidos por CKS y las normativas relevantes. Se documentarán los resultados de las pruebas y se tomarán medidas correctivas según sea necesario antes de la puesta en marcha completa de los sistemas restaurados.

e. Documentación y lecciones aprendidas

i. **Documentación detallada:** Registrar cada paso del proceso de recuperación de datos, incluyendo decisiones tomadas, tiempos de respuesta y resultados obtenidos.

ii. **Análisis post-recuperación**: Realizar un análisis post-recuperación para identificar áreas de mejora en los protocolos y procedimientos existentes.

iii. **Capacitación y sensibilización:** Capacitar al personal clave sobre los protocolos de recuperación de datos y difundir las lecciones aprendidas para mejorar la respuesta futura a incidentes similares.