

Copias de seguridad y restauración de OpenText

Content Server · Archive Center · Directory Services (OTDS)

Datos, documentos y configuración deben volver a funcionar juntos.

Proteger hoy
para garantizar la continuidad
del mañana.

1

QUÉ DEBEMOS PROTEGER

Los componentes clave de OpenText y su información.



Content Server

Base de datos, almacén documental y configuración.

Expedientes, permisos y referencias.



Archive Center

Base de datos, documentos archivados y contenido pendiente en búferes.

Búfer: zona temporal de recepción.



Identidad y conexiones

Datos y configuración de OTDS, integraciones, certificados y claves.

Usuarios, grupos y conectores (SAP, Microsoft 365, etc.).



Búsquedas

Copias de índices. Reconstruirlos puede llevar tiempo.

Independientes del contenido documental.

2

COPIAS COORDINADAS Y PROTEGIDAS

Un conjunto consistente y recuperable.

Entorno OpenText (en producción)

Content Server

Archive Center

Directory Services (OTDS)

Aplicaciones e integraciones

Configuración y certificados

Copias coordinadas

Datos, documentos y configuración

Almacenamiento de copias (separado y protegido)



Un conjunto recuperable

Bases de datos y archivos compatibles entre sí.



Copias cifradas y acceso restringido.



Una copia separada y desconectada.



Frecuencia y conservación acordadas.



No basta con copiar discos por separado.

Es necesario un conjunto coherente y recuperable.

3

RESTAURAR Y COMPROBAR

La única forma de saber que una copia sirve es probarla.

1



AISLAR

Preparar un entorno sin conexiones a producción.

2



RECUPERAR

Restaurar datos, documentos y configuración compatibles.

3



VALIDAR

Probar acceso, documentos, versiones, permisos y enlaces.

4



REGISTRAR

Guardar evidencias, resultado y tiempo empleado.



Archivo no es copia de seguridad

Archive Center también necesita respaldo.

El contenido puede estar pendiente en búferes y aún no en el archivo final.



Clúster no es copia de seguridad

La redundancia mejora la disponibilidad, pero no sustituye al respaldo.

Una avería, un error o un borrado pueden afectar a todos los nodos.

Copiar es el primer paso. Recuperar y comprobar es el objetivo.

SANTOSDOCASTRO
Conocimiento aplicado

Guía conceptual: ajustar el procedimiento a las versiones y al almacenamiento instalado.
Fuentes: OpenText — 3-0715, KB0798263, KB0829714 y Backup and recovery considerations. CISA — StopRansomware Guide.