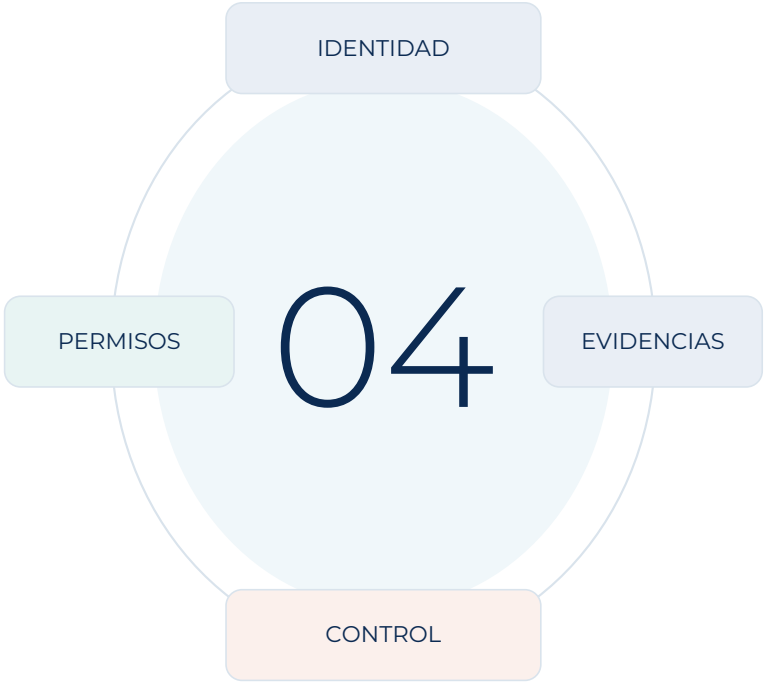



CUADERNO DE FORMACIÓN / MÓDULO 04

# SEGURIDAD DE OPENTEXT xECM




Definir accesos con criterio.
Proteger documentos e identidades.
Demostrar que las reglas se cumplen.

Siete fichas con explicaciones, modelos de acceso y ejercicios resueltos.
De la necesidad de negocio a la verificación de la seguridad efectiva.

**07**
FICHAS TEMÁTICAS

**21**
PÁGINAS DE DESARROLLO

**01**
CASO INTEGRADOR

Permisos · Usuarios, grupos y roles · ACL
OTDS + Active Directory · SSO
Workspaces · Verificación y buenas prácticas

Material didáctico independiente de SANTOSDOCASTRO. Casos y decisiones de ejemplo ficticios.




ANTES DE EMPEZAR / OBJETIVOS

# De la necesidad de acceso a una prueba reproducible

El objetivo es explicar quién puede hacer qué, dónde y por qué; también demostrar lo que debe quedar impedido.

### Al terminar, deberías poder…

Distinguir autenticación, autorización y trazabilidad. Relacionar una operación del negocio con el recurso y las identidades que intervienen, sin confundir SSO con acceso ilimitado.

### Diseñar y revisar un modelo de acceso

Traducir una matriz de responsabilidades a usuarios, grupos, roles y permisos. Identificar concesiones demasiado amplias y comprender los efectos de creación, copia, movimiento y propagación.

### Verificar el ciclo de vida completo

Seguir un alta, un cambio de función y una retirada. Comprobar las sesiones, las integraciones y el acceso efectivo de cuentas ordinarias, no solo el resultado con un administrador.

**A · Comprender**

Aprende la distinción entre las piezas. Antes de configurar nada, reformula la regla de seguridad con tus propias palabras.

**B · Aplicar**

Sigue una solución razonada del caso Bahía Ingeniería. Los esquemas y matrices son modelos didácticos, no capturas ni valores universales.

**C · Practicar**

Resuelve cuatro situaciones por ficha antes de consultar sus respuestas. Indica qué evidencia necesitarías para dar la situación por resuelta.

**Uso recomendado:** 6 horas orientativas, con ejercicios y debate. Requiere los módulos 1-3; no exige un sistema. Cualquier prueba técnica debe realizarse en un entorno autorizado y con datos ficticios.




ANTES DE EMPEZAR / ÍNDICE

# El recorrido del módulo

Cada ficha ocupa tres páginas: comprender, aplicar y practicar. Los títulos y el pie «Índice» son navegables.



**Para consolidar:** caso integrador, pp. 26-29; evaluación y soluciones, pp. 30-31; glosario, pp. 32-33; guía del formador, p. 34; ficha reutilizable de verificación, p. 35; referencias, pp. 36-37.




CASO TRANSVERSAL / BAHÍA INGENIERÍA

# El mismo expediente; ahora probamos sus fronteras

Los nombres, códigos, cuentas, tiempos y resultados de todos los ejercicios son ficticios.

## Lo que mantenemos de los módulos anteriores

Ana, de Compras, gestiona la información general del proveedor Talleres Bahía. Luis revisa los contratos desde Jurídico. Marta consulta las instrucciones operativas. Elena, de Tesorería, gestiona el certificado bancario.

## La restricción que debe seguir cumpliéndose

Entre esos perfiles de negocio, solo Elena tiene acceso al certificado. Ana, Luis y Marta no deben verlo ni descargarlo. Los borradores y las evidencias firmadas mantienen los accesos de la matriz del módulo 3, reproducida en la página 21.

## Qué añadimos para practicar

Diego administra accesos mediante una cuenta separada. Una revisora temporal participa en un contrato concreto. Algunos ejercicios simulan que Elena deja Tesorería: entonces se exige retirar también su acceso bancario, sin borrar el historial.

| DATOS DE REFERENCIA | |
|---|---|
| Origen del proveedor | ERP-PRO-100 |
| Proveedor | 0001042 · Talleres Bahía |
| Contrato principal | CT-2026-018 |
| Otro contrato | CT-2026-027 |
| Pedido | 4500000318 |
| Workspace proveedor | Node ID 31042 |
| Certificado del ejercicio | Node ID 71042 |

**Alcance:** el caso utiliza Content Server, xECM y OTDS. No fija una versión instalada ni una receta de configuración. La administración privilegiada se controla aparte; no es un acceso cotidiano de negocio.




# Permitir una tarea, no abrir todo el repositorio

La seguridad se define sobre una identidad, un recurso y una operación concreta.

## Empieza por la acción de negocio

Marta necesita consultar la instrucción de mantenimiento del contrato CT-2026-018. Eso no justifica que pueda modificarla, borrar sus versiones ni conceder acceso a otras personas. La petición correcta describe **qué contenido** necesita y **para qué operación**.

Content Server distingue permisos sobre los elementos y su contenido. El acceso que vemos en una pantalla puede resumir varios permisos detallados. Por eso una etiqueta como «colaborador» no basta para aprobar la configuración.

## Separa identidad, autorización y evidencia

Iniciar sesión identifica a Marta. Autorizar comprueba si esa identidad puede ejecutar la acción sobre el recurso. La trazabilidad permite reconstruir qué ocurrió. Son responsabilidades distintas.

En la prueba registra usuario, documento, operación y resultado. Comprueba la consulta permitida y, por separado, un intento de modificación que deba rechazarse. El éxito de la primera prueba no demuestra la segunda.

### Leer no es administrar

Poder abrir un documento no debe implicar poder cambiar sus accesos. La delegación de permisos es una responsabilidad adicional, no un premio por participar en el expediente.

### El recurso importa

El Workspace, sus carpetas y sus documentos requieren revisión propia. Ver el expediente no demuestra acceso a todo su contenido ni ausencia de accesos directos a un documento.

### Una evidencia no es un borrador

Una firma no configura por sí sola las restricciones del repositorio. La evidencia firmada necesita la política y los controles documentales previstos para evitar cambios ordinarios no autorizados.

**Pregunta de control:** ¿puedes expresar el acceso sin decir «que tenga permisos»? Por ejemplo: Marta consulta la instrucción de CT-2026-018, pero no la modifica ni administra su acceso.

[1] [2] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 26 / APLICAR

B · APLICAR

# Traducir operaciones a permisos verificables

Los nombres técnicos orientan la revisión; no sustituyen el diseño ni la ayuda de la versión instalada.

| Necesidad | Permisos que se revisan | Criterio aplicado al caso |
|---|---|---|
| Reconocer y consultar | **See** y **See Contents**. | Distinguir la visibilidad del elemento del acceso a su contenido. Marta debe abrir la instrucción autorizada, no el certificado bancario. |
| Cambiar la descripción | **Modify** y **Edit Attributes**, según los datos que se editen. | Ana mantiene la información general prevista. Comprueba por separado renombrado, propiedades y atributos; no los trates como una única acción. |
| Aportar y revisar contenido | **Add Items** en el destino; **Reserve** y **Add Major Version** cuando correspondan. | Luis revisa borradores. Prueba carga, reserva y nueva versión conforme al modelo de versionado; no otorgues control total para resolver una operación concreta. |
| Eliminar contenido o versiones | **Delete** y **Delete Versions**. | Eliminar un documento y eliminar una versión no son la misma necesidad. En este caso, la gestión ordinaria no autoriza a destruir evidencias firmadas. |
| Cambiar quién accede | **Edit Permissions**; revisar también la gestión del equipo. | La administración de accesos se asigna expresamente. Si Ana puede incorporar participantes a un rol, evalúa también qué accesos concede por esa vía. |

**No copies casillas a ciegas:** tipo de elemento, dependencias entre permisos, versionado y controles adicionales pueden cambiar el resultado. Valida la operación real con un perfil ordinario.

[1] [2] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 26 / PRACTICAR

C · PRACTICAR

# Practica: una acción permitida no autoriza las demás

Responde indicando identidad, recurso y operación. Evita la respuesta genérica «revisar seguridad».

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** Marta abre la instrucción, pero no puede sustituir su archivo. El equipo propone concederle control total. | Primero decide si Marta debe modificarla. La matriz solo le permite consultar. Si el negocio cambia esa necesidad, define el alcance y prueba el conjunto mínimo correspondiente, sin añadir administración ni borrado por comodidad. |
| **02.** Ana ve el nombre del certificado bancario aunque no puede descargarlo. ¿Se cumple la restricción del caso? | No. Para los perfiles no autorizados tampoco se ha previsto revelar ese elemento. Revisa la visibilidad, los metadatos y las otras rutas de consulta; una descarga rechazada no demuestra que toda la información esté protegida. |
| **03.** Luis modifica una descripción. ¿Eso demuestra que puede incorporar una nueva versión del borrador? | No. Son operaciones diferentes. Ejecuta una prueba autorizada de incorporación de versión, comprueba el resultado y revisa los permisos y el versionado aplicables. No deduzcas capacidades a partir de una etiqueta resumida. |
| **04.** La evidencia firmada solo tiene lectores ordinarios. ¿Se ha probado una inmutabilidad absoluta? | No. Has probado un alcance de acceso ordinario. Faltan los controles documentales, administrativos y de conservación que correspondan. Distingue protección frente a cambios cotidianos de una garantía absoluta sobre cualquier actor o mecanismo. |

**Criterio de aprendizaje:** una respuesta correcta limita el acceso a la tarea necesaria y evita convertir un permiso concreto en una capacidad universal.

[1] [2] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




# Persona, grupo y rol: tres decisiones distintas

Gestionar identidades y asignar responsabilidades son trabajos relacionados, pero no intercambiables.

## Una persona; una identidad trazable

La cuenta permite reconocer a Elena. Un grupo permite gestionar un conjunto de identidades con un criterio común. El rol del Workspace expresa una participación en un expediente, como Tesorería en el proveedor 0001042.

Pertenecer a un departamento no obliga a conceder todos sus accesos documentales. La asignación necesita una regla: quién la aprueba, a qué expedientes afecta y qué operaciones permite.

## El acceso tiene un ciclo de vida

En el alta se justifica la necesidad. En el cambio de puesto se revisan los accesos anteriores, no solo se añaden los nuevos. En la baja se comprueban las rutas por las que la cuenta aún podría actuar.

Para una colaboración temporal en CT-2026-018, asigna el alcance local necesario. No utilices el grupo de todos los contratos como atajo. Una fecha escrita en la solicitud no revoca nada sin un mecanismo o una tarea que la ejecute.

### Rol del Workspace

Relaciona una responsabilidad con participantes y permisos dentro del expediente. El nombre del rol no demuestra por sí mismo qué puede hacer cada participante.

### Rol de acceso de OTDS

Participa en el acceso al recurso integrado. No equivale al rol de negocio del Workspace ni reemplaza la autorización sobre cada documento.

### Cuenta técnica o privilegiada

Identifica una integración o una función administrativa. Requiere propietario responsable, alcance y control propios; no debe reutilizarse como identidad cotidiana compartida por el equipo.

**Comprobación:** explica qué cambia cuando Elena deja Tesorería. Deben revisarse grupos, roles locales, asignaciones directas y sesiones; quitar una sola etiqueta puede ser insuficiente.

[2] [4] [5] [7] [12] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 27 / APLICAR

B · APLICAR

# De la necesidad a una asignación con responsable

Este recorrido es un modelo de gobierno del caso, no una sincronización automática entre todas las cajas.

**01 Cuenta**

Elena tiene una identidad nominativa.

→

**02 Grupo**

Tesorería agrupa participantes autorizados.

→

**03 Rol local**

El grupo ocupa un rol en el proveedor 0001042.

→

**04 Operación**

El rol habilita tareas sobre el área Bancario.

## Alta que se puede explicar

El responsable de Tesorería solicita el acceso. El responsable del expediente confirma el alcance y Diego, administrador de accesos del caso, ejecuta el cambio con su cuenta administrativa.

La solicitud registra cuenta, grupo o rol, recurso, operaciones, motivo y revisión prevista. Elena comprueba su acceso; Marta sirve como contraste de un perfil que debe seguir excluido.

## Cambio que se puede cerrar

Cuando Elena deja la función, se identifican todas sus asignaciones relevantes. Se retiran las que ya no proceden y se revisan las sesiones y credenciales aplicables.

No se elimina el historial para simular que nunca trabajó allí. La evidencia de cierre demuestra el nuevo estado y mantiene atribuibles las actuaciones anteriores.

**Separación de responsabilidades:** el negocio justifica el acceso; la administración lo configura; la verificación comprueba el resultado. Una persona puede asumir varios papeles, pero deben quedar explícitos.

[2] [4] [5] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 27 / PRACTICAR

C · PRACTICAR

# Practica: evita accesos que sobreviven a la tarea

La pregunta no es solo quién entra hoy, sino por qué entra y cuándo debe dejar de hacerlo.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** Nuria revisará durante diez días un contrato. Se propone añadirla al grupo de todos los expedientes jurídicos. | Limita la asignación al contrato y a las operaciones necesarias. Registra quién aprueba, quién retira y cuándo se comprueba la retirada. La duración acordada exige una automatización validada o una tarea controlada, no solo una nota. |
| **02.** Un usuario tiene el rol de acceso de OTDS correcto. No abre el certificado. ¿Debes convertirlo en administrador? | No. El acceso al recurso integrado y el acceso al documento son distintos. Revisa la identidad reconocida, las asignaciones del Workspace y el permiso efectivo del certificado; contrasta antes si el negocio ha autorizado esa consulta. |
| **03.** Elena cambia de puesto. Se le añade al nuevo grupo sin revisar el anterior porque «ya la conocemos». | La confianza personal no sustituye la necesidad de acceso. Revisa sus concesiones de Tesorería, incluidas las locales y directas; conserva solo las justificadas por la nueva función. Comprueba la retirada con operaciones reales y evidencia fechada. |
| **04.** La integración utiliza la cuenta de Ana para que todos los registros tengan un nombre conocido. | Se confunde a la persona con el ejecutor técnico. Define una identidad de servicio o delegación soportada, con alcance controlado. La trazabilidad debe distinguir quién inició la acción y qué identidad la ejecutó realmente. |

**Criterio:** ninguna asignación debería quedar sin motivo, alcance, responsable y revisión. Los nombres de grupos y roles del caso son ejemplos, no valores estándar del producto.

[2] [4] [5] [7] [12] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




# Una ACL no se entiende mirando una sola fila

La lista de permisos configurados y el acceso efectivo responden a preguntas distintas.

## Reconoce todas las vías de acceso

Una ACL describe asignaciones de acceso al elemento. En Content Server deben revisarse las entradas aplicables: propietario, grupo propietario, acceso público y asignaciones a usuarios o grupos, además de los mecanismos del Workspace y controles del entorno.

Una asignación vacía para Marta no demuestra una prohibición efectiva. Podría obtener acceso mediante otro grupo o rol. No traslades a OpenText una regla de prioridad de denegaciones aprendida en otro sistema.

## Distingue cuatro momentos

La creación puede tomar permisos de un origen configurado. Una aplicación a descendientes cambia un conjunto existente. Mover o copiar introduce un nuevo destino. La sincronización continua, si existe, es otro mecanismo.

No son equivalentes. Define el alcance de la operación y revisa las excepciones antes de ejecutarla. Cambiar la plantilla tampoco demuestra que se hayan corregido todos los expedientes ya creados.

### Configurado no es efectivo

La ACL explica concesiones. La consulta de permisos efectivos y las pruebas con el usuario ayudan a comprobar su resultado. La causa de un acceso inesperado debe quedar identificada.

### Public Access requiere revisión

No significa automáticamente un enlace anónimo de Internet. Es una vía de acceso del repositorio cuyo alcance debe comprobarse; no es apropiada para abrir el área bancaria del caso.

### Propagar puede borrar excepciones

Una aplicación masiva sobre descendientes puede afectar contenido restringido. Selecciona el alcance, conserva la configuración anterior y prueba una muestra que incluya esas excepciones.

**Regla de razonamiento:** «sin acceso previsto» en una matriz es un requisito. No significa que debas crear una entrada técnica de denegación ni que esa entrada vaya a prevalecer.

[1] [2] [3] [6] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 28 / APLICAR

B · APLICAR

# Localiza la concesión que abre la puerta

Marta descarga el certificado 71042. El nombre Bancario y una entrada individual vacía no la detienen.

| Vía detectada | Situación del ejercicio | Tratamiento razonado |
|---|---|---|
| Rol Tesorería | Elena tiene las operaciones bancarias previstas. | Conservar el acceso necesario. La corrección de una exposición no debe impedir el trabajo autorizado sin plan alternativo. |
| Grupo TodoPersonal | Una concesión amplia permite consultar el certificado; Marta pertenece al grupo. | Retirar esa concesión del contenido restringido y revisar los descendientes afectados. No quitar a Marta de toda la organización como atajo. |
| Entrada individual Marta | No concede operaciones adicionales. | No neutraliza por sí sola la vía del grupo. Comprueba el resultado efectivo sin inventar una regla universal de prioridad. |
| Propietario y otras asignaciones | Aún no se han revisado. | Inspeccionar el propietario, su grupo y el resto de concesiones. Un informe incompleto no permite cerrar la incidencia. |

**Después del cambio:** prueba el certificado existente y uno nuevo creado en Bancario. Elena conserva las operaciones previstas; Ana, Luis y Marta no ven ni descargan el contenido restringido. Repite la comprobación por enlace directo autorizado de prueba.

**Antes de propagar:** define qué elementos cambiarán, conserva su estado anterior y protege las excepciones. Un resultado correcto en la carpeta superior no demuestra el de todos sus documentos.

[1] [2] [3] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 28 / PRACTICAR

C · PRACTICAR

# Practica: crear, mover y propagar no son lo mismo

Razonar la herencia exige indicar el momento, el origen, el destino y los elementos afectados.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** Se quitan permisos a Marta en una fila individual, pero sigue accediendo mediante TodoPersonal. | La retirada no ha eliminado la vía efectiva del grupo. Identifica todas las concesiones aplicables y corrige la incompatible con el recurso restringido. No supongas que la entrada individual vacía equivale a una denegación que prevalece. |
| **02.** Se cambia la ACL de una plantilla y se informa de que los 200 expedientes anteriores ya están corregidos. | No se ha demostrado. Distingue futuros expedientes de los existentes. Inventaría los afectados, define una corrección controlada y valida una muestra representativa, incluidas excepciones. La cifra de 200 es un dato del ejercicio, no una prueba de propagación. |
| **03.** Se mueve el certificado a General y se devuelve a Bancario. ¿Puede ignorarse el movimiento porque ya está en su sitio? | No. Hay que revisar los permisos resultantes y si durante el movimiento existió acceso no previsto. Conserva las evidencias y sigue el procedimiento de incidente si hubo exposición. Volver a la ruta original no prueba que todo se haya deshecho. |
| **04.** Se aplicarán permisos a todos los descendientes. La muestra de prueba contiene solo documentos generales. | La muestra no cubre el mayor riesgo: perder restricciones especiales. Incluye Bancario, evidencias firmadas y cualquier excepción relevante. Define copia de configuración, alcance y reversión antes de ejecutar el cambio; comprueba también el contenido nuevo. |

**Criterio:** describe la concesión que realmente cuenta. Si solo nombras el padre o la plantilla, todavía no has demostrado el acceso del documento.

[1] [2] [3] [6] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 29 / COMPRENDER

A · COMPRENDER

# Del directorio al repositorio: sigue la identidad

Sincronizar cuentas no equivale a autenticar sesiones ni a autorizar documentos.

## Cada sistema tiene una responsabilidad

En este caso, Active Directory mantiene las identidades corporativas y sus grupos. OTDS integra esa información con los recursos OpenText según la configuración. Content Server debe reconocer la identidad que finalmente utiliza el repositorio.

El nombre visible no basta para enlazar cuentas. Deben definirse identificadores, particiones y reglas de correspondencia. Dos cuentas llamadas Elena pueden representar identidades distintas; un cambio de correo no debería resolverse creando duplicados sin análisis.

## El cambio necesita un recorrido completo

Cuando Elena deja Tesorería, el cambio en el origen tiene que llegar a los componentes que lo utilizan. Después se revisan permisos locales y sesiones. La prueba debe mostrar el estado final, no solo un mensaje de sincronización correcta.

No deduzcas que sincronizar usuarios implica copiar sus contraseñas ni que un retraso se arregla ampliando permisos. Primero identifica qué tramo está pendiente y qué dato falta.

### Partición

Organiza identidades dentro de OTDS. Puede formar parte de una configuración sincronizada o no sincronizada. Su nombre y sus reglas ayudan a distinguir el origen de una cuenta.

### Recurso integrado

Representa la aplicación conectada. Ver a Elena en OTDS no demuestra que la cuenta y sus grupos estén correctamente disponibles en el recurso Content Server previsto.

### Conexión y filtros

El alcance de sincronización, las credenciales de conexión y el canal protegido se revisan conjuntamente. Importar todo el directorio o desactivar validaciones no son soluciones neutrales.

**Pregunta de control:** ¿en qué sistema se aprobó el cambio, dónde se observa ya y dónde falta? Una captura de Active Directory no acredita por sí sola el estado de Content Server.

[4] [5] [9] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 29 / APLICAR

B · APLICAR

# Una baja se cierra con evidencia de extremo a extremo

Los tiempos de esta secuencia son ficticios: ilustran una comprobación, no una latencia garantizada del producto.

**Active Directory**

Cambio de cuenta o pertenencia en el origen.

→

**OTDS**

Estado e identidad en la partición correcta.

→

**Content Server**

Cuenta efectiva, grupos, roles y acceso al recurso.

| Observación | Evidencia recogida | Qué falta para cerrar |
|---|---|---|
| 09:00 - Origen | Se retira a Elena de Tesorería. | Confirmar que el cambio llega al destino y no existe otra concesión. |
| 09:04 - OTDS | La pertenencia ya no aparece en la partición esperada. | Revisar el recurso Content Server; no basta con ver el cambio en OTDS. |
| 09:06 - Repositorio | El grupo actualizado no concede ya la tarea bancaria. | Revisar asignaciones directas, roles locales y sesiones previas. |
| 09:08 - Prueba funcional | Un acceso de prueba desde una sesión anterior aún funciona. | La retirada no está demostrada. Tratar la sesión según el mecanismo soportado y volver a verificar. |

**Resultado exigible:** confirmar tanto el rechazo de nuevos accesos como el tratamiento de sesiones anteriores. Mide la ventana observada y registra el cierre; no inventes un plazo universal de revocación.

[4] [5] [9] [10] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 29 / PRACTICAR

C · PRACTICAR

# Practica: localiza el tramo, no inventes la causa

Diferencia evidencia del origen, de la sincronización, del recurso y de la sesión.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** El directorio muestra la baja, pero Elena todavía consulta desde una sesión abierta. ¿Puede cerrarse la tarea? | No. Comprueba el estado recibido por OTDS y Content Server, las concesiones locales y el tratamiento de sesiones. La captura del origen solo acredita un tramo. Conserva hora, identidad y resultado de las pruebas hasta demostrar la retirada efectiva. |
| **02.** Hay dos cuentas llamadas Elena. El equipo propone unirlas porque el nombre coincide. | El nombre no es una identidad fiable. Contrasta identificadores de origen, partición y correspondencia con el recurso. Revisa también la atribución histórica antes de consolidar o eliminar nada; una unión equivocada puede transferir accesos. |
| **03.** Un problema de certificado impide la conexión al directorio. Se propone desactivar la validación permanentemente. | Corrige confianza, nombre, vigencia o cadena del certificado según el error demostrado. Desactivar la validación rebaja la protección y no arregla su causa. Trabaja con el responsable de identidad y prueba la conexión protegida. |
| **04.** La sincronización de grupos ha terminado bien. ¿Se ha probado que las contraseñas se copian y que el SSO funciona? | No. El aprovisionamiento de identidades, el mecanismo de autenticación y el SSO son distintos. Revisa el diseño y ejecuta cada prueba por separado. No infieras el tratamiento de credenciales a partir de una actualización de grupos. |

**Criterio:** en cada respuesta debe aparecer una evidencia concreta del siguiente tramo. «Esperar un rato» o «dar más permisos» no sustituyen el diagnóstico.

[4] [5] [9] [10] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 30 / COMPRENDER

A · COMPRENDER

# SSO: iniciar sesión sin repetir la autenticación

El inicio de sesión único mejora la experiencia de autenticación; no convierte al usuario en administrador.

## La confianza sustituye pasos repetidos

En un esquema federado, una aplicación confía en información de autenticación emitida por un proveedor de identidad. OTDS puede participar en esa integración. La aplicación reconoce a la persona y mantiene el contexto de sesión que corresponda.

El diseño concreta el mecanismo soportado, los extremos que confían entre sí y la correspondencia de cuentas. No basta con que dos aplicaciones utilicen el mismo nombre de usuario.

## Tres cosas que no deben confundirse

SSO evita repetir ciertos pasos de autenticación. MFA añade factores para verificar la identidad. La autorización decide qué puede hacer esa identidad sobre cada recurso.

Marta puede completar correctamente el SSO y tener que recibir una negativa al abrir el certificado. Ese rechazo es el comportamiento esperado del caso. También deben distinguirse las sesiones del proveedor de identidad, OTDS y la aplicación; cerrar una no demuestra que todas queden invalidadas.

### SAML y OpenID Connect

Son mecanismos que pueden intervenir en la federación de identidad. La selección y compatibilidad dependen del diseño. Este módulo no prescribe un protocolo universal de xECM.

### ID token y access token

En OpenID Connect, el ID token comunica información de autenticación al cliente. Un access token sirve para acceder a un recurso según su validación. No son intercambiables por tener forma parecida.

### Una sesión no es una contraseña

Cookies, tickets y tokens pueden permitir continuar una sesión. Deben protegerse y tratarse conforme a su emisor y consumidor; cambiar la contraseña no prueba por sí solo su revocación.

**Resultado correcto:** Marta entra con su identidad real y consulta lo previsto. El certificado sigue protegido. «No ha pedido otra contraseña» es solo una parte de la prueba.

[4] [5] [7] [8] [9] [10] [14] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 30 / APLICAR

B · APLICAR

# Sigue el acceso y distingue cada validación

Secuencia conceptual: no representa todos los intercambios ni el orden interno de cualquier implantación.

**01 Solicitud**

Marta solicita una aplicación protegida.

→

**02 Identidad**

El proveedor verifica o reconoce su sesión.

→

**03 Confianza**

El receptor valida el mensaje y la identidad.

→

**04 Sesión**

La aplicación establece su contexto local.

→

**05 Permiso**

El recurso decide si la acción está autorizada.

## Prueba positiva y prueba negativa

Marta entra por el recorrido publicado y abre la instrucción de mantenimiento. Después intenta el acceso de prueba al certificado: el sistema debe impedir la consulta y la descarga.

Registra la identidad que reconoce Content Server. Que el portal muestre «Marta» no demuestra que una integración posterior no esté actuando con una cuenta de servicio más potente.

## Prueba de confianza y cierre

En laboratorio, revisa que el recorrido rechace credenciales o mensajes no válidos conforme al mecanismo implantado. Comprueba emisor, destinatario, vigencia y confianza donde correspondan.

Ensaya después el cierre y la retirada con una sesión nueva y otra preexistente. Documenta qué componente invalida cada contexto; no presupongas un cierre global automático.

**No mezcles problemas:** un fallo de confianza del SSO no se resuelve ampliando la ACL del documento. Una denegación documental prevista no se resuelve relajando la autenticación.

[4] [5] [7] [8] [9] [10] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




# Practica: entrar bien y quedar correctamente limitado

Identifica si el problema está en la autenticación, en la sesión o en la autorización del recurso.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** Marta supera la autenticación multifactor, pero no abre el certificado bancario. El equipo lo considera un error. | No lo es según la matriz del caso. MFA refuerza la verificación de identidad; no concede acceso bancario. Comprueba que Marta abre el contenido operativo permitido y que el certificado queda correctamente fuera de su alcance. |
| **02.** La sesión del proveedor de identidad se cierra. ¿Es suficiente para afirmar que Content Server no aceptará ninguna sesión anterior? | No. Revisa el mecanismo de cierre o revocación y la sesión mantenida por la aplicación. Realiza una prueba controlada con un contexto anterior. Documenta los resultados reales en lugar de equiparar todos los estados de sesión. |
| **03.** Tras renovar un certificado, falla el SSO de todos. Se propone abrir Public Access para que puedan trabajar. | Eso no corrige la confianza y puede exponer contenido. Comprueba el cambio de certificado, la configuración de confianza y las validaciones del recorrido. Usa el procedimiento de contingencia autorizado; no cambies la política documental para ocultar el fallo. |
| **04.** El portal enseña el nombre de Marta, pero descarga con una cuenta que lee todos los documentos. | La identidad visual no limita al ejecutor técnico. Verifica cómo se autoriza el recurso solicitado y con qué identidad se recupera. Una integración debe preservar o aplicar los controles necesarios antes de entregar contenido al usuario. |

**Criterio:** separa comodidad de acceso, garantía de identidad, autorización y duración de sesión. Son cuatro preguntas, no una sola casilla de SSO.

[4] [5] [7] [8] [9] [10] [14] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 31 / COMPRENDER

A · COMPRENDER

# El Workspace conecta trabajo, no elimina fronteras

Compartir contexto de negocio no obliga a compartir todos sus documentos ni las facultades de administrarlos.

## Parte de la matriz, no de la carpeta

El proveedor 0001042 agrupa información general y bancaria. Sus contratos tienen expedientes propios. Las relaciones facilitan navegar, pero no justifican transferir al destino todos los accesos del origen.

La matriz del caso debe traducirse a roles, participantes, permisos y excepciones verificables. Si un rol amplio alcanza Bancario, renombrar la carpeta o esconder su widget no resuelve la incompatibilidad.

## Prueba el contenido y su evolución

Comprueba el expediente existente y uno creado con la plantilla vigente. Incluye documentos recién aportados, movimientos y cambios del equipo. La seguridad que funcionaba ayer puede dejar de corresponder al modelo después de una operación.

Identifica quién puede modificar participantes y accesos. Un coordinador de trabajo no necesita por ello ampliar la audiencia bancaria. La administración privilegiada, cuando proceda, se trata como acceso excepcional y controlado, no como participación ordinaria de negocio.

### Plantilla e instancia

Revisa por separado los permisos de la plantilla, las reglas de creación y los Workspaces ya existentes. Una corrección del modelo no acredita el resultado de todas las instancias.

### Cada canal cuenta

Incluye interfaz, búsqueda, enlace directo y API cuando formen parte del alcance. Comprueba también títulos, atributos y vistas previas: una fuga no se limita al archivo completo.

### La copia sale de esa frontera

Una descarga o un adjunto puede generar otra copia fuera del repositorio. Retirar permisos no garantiza su borrado remoto. La entrega externa necesita su propia política y controles.

**Prueba crítica:** Elena mantiene la operación bancaria prevista; Ana, Luis y Marta no acceden al certificado. La restricción debe resistir cambios de vista, nuevas cargas y accesos por rutas alternativas.

[1] [2] [3] [6] [7] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 31 / APLICAR

B · APLICAR

# Una matriz que el equipo puede poner a prueba

Se conserva la matriz de negocio del módulo 3. Las letras son requisitos, no nombres de permisos técnicos.

| Área o contenido | Ana Compras | Luis Jurídico | Marta Operaciones | Elena Tesorería |
|---|---|---|---|---|
| Proveedor: documentos generales | G | C | - | C |
| Proveedor: certificado bancario | - | - | - | G |
| Contrato: borradores de negociación | C | G | - | - |
| Contrato: evidencia firmada | C | C | C | C |
| Contrato: instrucciones operativas | G | C | C | - |

**C:** consultar. **G:** aportar y modificar contenido conforme a su política; no incluye administrar accesos ni alterar evidencias firmadas. **-:** sin acceso previsto; no representa una entrada de denegación.

**Prueba completa:** para cada perfil ejecuta una operación permitida y otra no permitida. Comprueba tanto el documento actual como uno nuevo en la misma área. La gestión de equipos y el acceso administrativo se validan en pruebas separadas.

> **Regla del caso:** entre los perfiles de negocio, el certificado pertenece al ámbito de Tesorería. Un enlace desde el contrato no amplía esa audiencia ni autoriza a duplicarlo en un área general.

[1] [2] [6] [7] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 31 / PRACTICAR

C · PRACTICAR

# Practica: la restricción debe sobrevivir a los cambios

Utiliza la matriz de la página anterior como criterio de aceptación.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** El certificado no aparece en el widget, pero Marta lo localiza por búsqueda y descarga desde el resultado. | La restricción no se cumple. Investiga visibilidad y permisos del recurso, además de la identidad efectiva del canal. Ocultar el widget no protege los resultados de búsqueda ni la descarga; contiene la exposición y repite las pruebas. |
| **02.** Un nuevo documento bancario resulta visible para Ana, aunque el certificado antiguo está protegido. | La prueba del documento antiguo no cubría la creación. Revisa el origen de permisos del contenido nuevo, su propietario y las reglas de plantilla o destino. Corrige el proceso de alta y los documentos afectados, no solo el ejemplo antiguo. |
| **03.** El Workspace del contrato se relaciona con el proveedor. Se propone que todos sus lectores vean también Bancario. | La relación da contexto, no una justificación de negocio para ampliar la audiencia. Mantén la restricción de Tesorería y comprueba el acceso al destino. Un usuario puede navegar entre asuntos sin tener acceso a todos sus documentos. |
| **04.** Elena envió una copia por correo. Después se retira el acceso al original y se afirma que nadie conservará el archivo. | No puede afirmarse. El cambio controla el acceso al repositorio, no demuestra la eliminación de copias externas. Revisa la entrega según la política y el procedimiento de incidente que corresponda, sin prometer una revocación remota inexistente. |

**Criterio:** una frontera documental se comprueba sobre recursos y operaciones, no por el nombre del contenedor, la perspectiva ni la aplicación desde la que se llega.

[1] [2] [3] [6] [7] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




# La seguridad se mantiene, no se entrega una sola vez

Una ACL correcta puede convivir con una integración demasiado potente, un secreto expuesto o una restauración mal validada.

## Extiende el control al recorrido real

El diseño debe abarcar personas, cuentas de servicio, administración, comunicaciones y destinos de la información. Reutiliza las fronteras de DEV, PRE y PRO del módulo 2: una prueba no debe acceder a documentos o identidades reales por una configuración heredada.

Una integración no se justifica diciendo que «necesita funcionar». Define operaciones, recursos, identidad ejecutora y modo de comprobar la autorización del solicitante. La cuenta técnica no debe convertirse en un acceso indiscriminado al repositorio.

## Prepara cambios y recuperación

Antes de una modificación masiva de permisos, identifica alcance, aprobación, estado anterior y verificación posterior. Conserva también un mecanismo de vuelta atrás compatible con las restricciones actuales.

Tras restaurar, revisa identidades y accesos antes de reabrir el servicio. Recuperar una configuración antigua puede reintroducir una concesión que ya se había retirado. La prueba funcional necesita ir acompañada de una prueba de seguridad.

### Secretos con ciclo de vida

Credenciales, claves y tokens requieren almacenamiento protegido, acceso limitado y sustitución controlada. Evita exponerlos en capturas, código, material formativo o registros operativos.

### Trazabilidad que sirva

Define los sucesos relevantes y cómo correlacionarlos: quién, qué recurso, qué operación, cuándo y con qué resultado. Un registro sin contexto no permite reconstruir el cambio.

### Comprobar sin exponer

Utiliza datos ficticios y cuentas de prueba en un entorno autorizado. Las evidencias deben demostrar el resultado sin incluir contraseñas, tokens ni el contenido bancario real.

**Objetivo:** convertir cada control en una responsabilidad y una prueba. «Tenemos SSO», «está cifrado» o «hay logs» no acreditan por sí solos el recorrido completo.

[7] [9] [10] [11] [12] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 32 / APLICAR

B · APLICAR

# Del control escrito a una evidencia comprobable

Cada fila propone una prueba del caso. La periodicidad y el procedimiento se acuerdan con los responsables del servicio.

| Control | Aplicación en Bahía Ingeniería | Evidencia de verificación |
|---|---|---|
| Acceso mínimo | Separar cuenta cotidiana, administración e integración. Limitar cada una a su función. | Pruebas permitidas y no permitidas con la identidad efectiva de cada recorrido. |
| Secreto protegido | Mantener la credencial técnica fuera del código y los logs; ensayar su sustitución. | La credencial nueva funciona; la anterior deja de ser aceptada según el procedimiento validado. |
| Canal y confianza | Proteger las comunicaciones y validar la confianza; no resolver errores desactivando comprobaciones. | Prueba del recorrido protegido y rechazo esperado de una configuración no válida en laboratorio. |
| Cambio y auditoría | Aprobar alcance, guardar el estado previo y registrar el cambio de grupos, roles o ACL. | Solicitud vinculada al ejecutor, elementos afectados, momento y resultado; sin secretos en el registro. |
| Retirada y recuperación | Comprobar sesiones antiguas y nuevas. Revisar permisos después de restaurar. | La restricción de Bancario y las bajas vigentes siguen cumpliéndose antes de reabrir el servicio. |

**Seguridad y operación:** una corrección debe mantener el trabajo autorizado y cerrar el acceso indebido. Guarda evidencias de ambos resultados; una indisponibilidad total no equivale a una solución sostenible.

[7] [9] [10] [11] [12] [13] [14] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




FICHA 32 / PRACTICAR

C · PRACTICAR

# Practica: no confundas una promesa con un control

Explica la medida, su responsable y la prueba que permitiría darla por implantada.

| Resuelve antes de mirar | Solución razonada |
|---|---|
| **01.** Un token aparece en un log enviado a soporte. Se elimina la línea del fichero local y se cierra la incidencia. | No basta: pueden existir copias del log. Trata la credencial como expuesta, aplica la revocación o sustitución prevista y revisa el alcance. Corrige el registro para no repetirlo y conserva evidencias sin volver a incluir el secreto. |
| **02.** Después de restaurar una copia antigua, Elena vuelve a aparecer en Tesorería. La aplicación abre correctamente. | La recuperación funcional no acredita seguridad. Reconcilia identidades, roles y permisos con las retiradas vigentes antes de reabrir. Repite la prueba del certificado y documenta cómo se evita que la restauración reintroduzca el acceso retirado. |
| **03.** La integración devuelve documentos por su identificador. El equipo supone que nadie conocerá los identificadores restringidos. | El identificador no es una autorización. El recorrido debe comprobar el acceso del solicitante al recurso antes de entregarlo. Usa dos documentos ficticios, uno permitido y otro restringido, y valida que el segundo no se revela. |
| **04.** La auditoría registra solo «operación correcta». No guarda actor, objeto ni correlación con la solicitud. | Ese dato no permite atribuir ni reconstruir el cambio. Define los campos necesarios y una prueba de búsqueda de evidencias. Protege los registros y limita su contenido: más datos no es mejor si se incorporan secretos o información innecesaria. |

**Criterio:** la medida debe cerrar la causa o el riesgo demostrado, no solo hacer desaparecer el síntoma de una pantalla.

[7] [9] [10] [11] [12] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




CASO INTEGRADOR / ENUNCIADO

# Antes de aprobar la seguridad del proveedor

Trabajo propuesto: 35 minutos. Utiliza la matriz de la página 21 y presenta una solución que pueda comprobarse.

## Los hechos que llegan a revisión

El certificado 71042 se puede descargar con la cuenta de Marta porque conserva una concesión del grupo TodoPersonal. El propietario del documento es una cuenta de carga cuya capacidad no se ha revisado.

La plantilla ya se ha corregido, pero hay 200 Workspaces anteriores sin verificación. Elena ha dejado Tesorería y conserva una sesión desde la que todavía consulta el certificado.

## El recorrido que faltaba probar

El portal muestra el nombre del usuario, pero recupera archivos con una cuenta técnica de acceso amplio sin demostrar la autorización del solicitante. Una traza enviada a soporte contiene un token.

La aprobación se basaba en pruebas hechas solo con un administrador. Mañana se ensayará una restauración de una copia anterior a los cambios de acceso.

### 01 · Modelo y prioridades

Señala los accesos que no cumplen la matriz y qué exposiciones deben contenerse primero. Distingue hechos de aspectos todavía no revisados.

### 02 · Plan de corrección

Define acción, responsable y alcance. Trata los expedientes existentes, las altas futuras, las sesiones, la integración y la credencial expuesta.

### 03 · Pruebas y cierre

Propón ocho comprobaciones con identidad, recurso, operación y resultado. Explica qué debe validarse tras la restauración y quién acepta el cierre.

**Entrega:** un modelo de accesos, un plan priorizado, ocho pruebas y un registro de decisiones pendientes. No se piden comandos ni una corrección improvisada sobre producción.




CASO INTEGRADOR / SOLUCIÓN RAZONADA

# Corregir la causa sin perder el control del cambio

Se admiten diseños alternativos si preservan la matriz, cierran la exposición y aportan evidencias equivalentes.

### 01 · Contener el acceso al certificado

El responsable del contenido y seguridad delimitan la exposición. Se corrige la concesión de TodoPersonal sobre el recurso restringido y se revisan propietario y otras vías. Se conserva la evidencia del incidente; no se elimina el documento para ocultar el problema.

### 02 · Separar plantilla e instancias

La plantilla corregida sirve para comprobar nuevas altas. Los 200 expedientes necesitan inventario, alcance de corrección y control de excepciones. La verificación debe cubrir el conjunto afectado y pruebas funcionales representativas; una muestra no prueba por sí sola los 200.

### 03 · Completar la retirada de Elena

Identidad y administración documental revisan origen, OTDS, recurso, grupos y roles locales. Se tratan las sesiones conforme a mecanismos soportados. El cierre demuestra rechazo de nuevos accesos y de contextos anteriores pertinentes, sin alterar las atribuciones históricas.

### 04 · Corregir la frontera del portal

El responsable de integración identifica al solicitante real y valida su autorización antes de entregar documentos. Revisa la delegación soportada o el control explícito necesario. El acceso de la cuenta técnica no puede convertirse en acceso de todos los usuarios.

### 05 · Tratar el token como expuesto

El responsable de la credencial aplica la revocación o sustitución prevista, evalúa las copias de la traza y corrige el registro. Conserva la evidencia del tratamiento sin incluir el secreto. Borrar una línea local no cierra el alcance de la exposición.

### 06 · Validar antes de reabrir

La restauración se reconcilia con la política actual y las retiradas vigentes. Se prueban cuentas ordinarias, canales de acceso y credenciales. Negocio valida su matriz; seguridad y operación aceptan controles y riesgos pendientes de forma explícita.

**Conclusión modelo:** no aprobar el estado observado. La aprobación posterior requiere evidencias del acceso autorizado, de las restricciones y de la retirada; no basta con que la pantalla vuelva a funcionar.

[1] [2] [7] [9] [10] [11] [12] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




CASO INTEGRADOR / PRUEBAS DE ACEPTACIÓN

# Ocho comprobaciones con un resultado observable

Define las cuentas de ensayo, la versión y los canales disponibles. No registres contraseñas ni tokens en las evidencias.

### 01 · Acceso permitido

Elena, antes del cambio de función, abre el certificado por las rutas previstas. Guardar cuenta, nodo, versión, hora y resultado de consulta.

### 02 · Acceso excluido

Ana, Luis y Marta no ven ni descargan el certificado. Comprobar interfaz, búsqueda y acceso directo del ensayo; conservar resultados de cada identidad.

### 03 · Contenido nuevo

Crear un documento bancario y un Workspace de prueba con el modelo vigente. Verificar que no aparecen concesiones amplias ni acceso indebido del creador.

### 04 · Expedientes anteriores

Reconciliar el inventario de 200 instancias con el cambio aplicado. Revisar excepciones y muestras funcionales; dejar identificados fallos, pendientes y cobertura real.

### 05 · Retirada efectiva

Tras la salida de Elena de Tesorería, verificar identidades, concesiones y sesiones antiguas y nuevas. Registrar el momento observado del rechazo y el cierre.

### 06 · Integración y API

Con Marta como solicitante, entregar la instrucción permitida y rechazar el certificado. Acreditar identidad solicitante, ejecutor técnico y autorización aplicada al recurso.

### 07 · Secreto y auditoría

Verificar la sustitución o revocación del token expuesto. Localizar el evento de cambio con actor y objeto, sin reproducir el secreto en ningún registro.

### 08 · Restauración segura

Antes de reabrir, comprobar que la copia restaurada no reintroduce el grupo amplio ni el acceso retirado. Conservar reconciliación, pruebas y aceptación final.

**Una denegación debe demostrar falta de acceso:** una caída general o un error indeterminado no acreditan la política. Contrasta un recurso permitido y otro restringido con el mismo recorrido.

[1] [7] [9] [10] [11] [12] [13] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




CASO INTEGRADOR / CORRECCIÓN Y CIERRE

# Cómo valorar la solución y justificar la decisión

Rúbrica formativa de 10 puntos. Evalúa el razonamiento y la evidencia, no la cantidad de terminología empleada.

| Dimensión | Para obtener 2 puntos debe quedar explicado | Puntos |
|---|---|---|
| Modelo de acceso | La solución respeta la matriz y separa identidad, recurso, operación y administración. | 0 / 1 / 2 |
| Concesiones y alcance | Identifica la vía del grupo amplio, el propietario y el tratamiento diferenciado de plantilla e instancias. | 0 / 1 / 2 |
| Ciclo de identidad | Sigue la retirada entre sistemas y comprueba sesiones antiguas y nuevas, sin suponer revocación instantánea. | 0 / 1 / 2 |
| Integración y secretos | La entrega de documentos valida al solicitante; el token expuesto se trata y la auditoría evita reproducirlo. | 0 / 1 / 2 |
| Pruebas y recuperación | Propone comprobaciones permitidas y no permitidas, cobertura del cambio y revisión de seguridad tras restaurar. | 0 / 1 / 2 |

**Escala:** 0 = ausente o incorrecto; 1 = parcial o sin evidencia; 2 = correcto y justificado. La puntuación orienta el repaso y no constituye una certificación ni una aceptación de producción.

**Acta de cierre:** registrar responsable, alcance realmente verificado, incidencias abiertas, riesgos aceptados por quien tenga autoridad y fecha de revisión. Lo que no se ha probado se mantiene como pendiente.

> **Condición no compensable por la nota:** si Marta sigue accediendo al certificado o no se ha demostrado la retirada de Elena, la restricción del caso permanece incumplida aunque otros apartados estén bien resueltos.




EVALUACIÓN / RESPONDE SIN CONSULTAR

# Diez preguntas para explicar una decisión

Dedica 15 minutos. Responde con frases completas y añade una comprobación concreta cuando corresponda.

### 01 · Permiso y operación

Marta consulta una instrucción. ¿Por qué no debes deducir que puede modificarla o conceder acceso a otro usuario?

### 02 · Usuario, grupo y rol

Explica con Elena la diferencia entre cuenta, grupo corporativo, rol del Workspace y rol de acceso de OTDS.

### 03 · Acceso efectivo

Marta no tiene una concesión individual, pero pertenece a un grupo con lectura. ¿Qué debes revisar antes de afirmar que no accede?

### 04 · Herencia y cambio

¿Por qué corregir una plantilla no demuestra que todos los documentos de los expedientes anteriores estén ya protegidos?

### 05 · Directorio y repositorio

Una baja figura en Active Directory. ¿Qué otros estados y pruebas necesitas para acreditar la retirada documental?

### 06 · SSO y MFA

¿Puede un usuario superar SSO y MFA y, correctamente, no tener acceso a un documento? Explica la diferencia.

### 07 · Sesiones

¿Por qué cerrar la sesión del proveedor de identidad no prueba que todos los contextos de la aplicación hayan quedado invalidados?

### 08 · Canales y copias

¿Qué distingue ocultar un widget, retirar acceso al documento y tratar una copia que ya se ha enviado por correo?

### 09 · Integración

El portal muestra a Marta, pero descarga mediante una cuenta técnica. ¿Qué autorización debe quedar demostrada antes de entregar el contenido?

### 10 · Recuperación

Tras restaurar, la aplicación abre bien. ¿Qué riesgo de seguridad puede persistir y qué comprobarías antes de reabrir?

**Autocorrección:** un punto por respuesta correcta y razonada. Si confundes autenticación con permisos o no puedes explicar una retirada efectiva, revisa esas fichas aunque el total sea alto.




EVALUACIÓN / SOLUCIONES

# La explicación importa más que la etiqueta

Estas respuestas expresan el razonamiento mínimo. Las referencias de página indican dónde ampliar cada concepto.

**01 · Operaciones distintas · pp. 5-7**

Consultar, modificar y administrar accesos son tareas diferentes. Cada una requiere justificación y comprobación propia sobre el recurso concreto.

**02 · Cuatro funciones · pp. 8-10**

La cuenta identifica; el grupo agrupa; el rol del Workspace organiza participación local; el de OTDS participa en acceso al recurso integrado.

**03 · Todas las concesiones · pp. 11-13**

Revisa grupos, roles, propietario y demás asignaciones aplicables, y contrasta el acceso efectivo. Ausencia de concesión individual no demuestra exclusión.

**04 · Modelo e instancias · pp. 11-13**

La corrección del modelo y el cambio sobre contenido existente son operaciones distintas. Hace falta inventario, alcance, ejecución y verificación de afectados.

**05 · Recorrido completo · pp. 14-16**

Comprueba OTDS, recurso, grupos y roles locales, y sesiones anteriores y nuevas. La evidencia del origen no acredita el resultado final.

**06 · Identidad y permiso · pp. 17-19**

Sí. SSO y MFA tratan la autenticación; la autorización del documento conserva sus límites. El certificado debe seguir excluido para Marta.

**07 · Contextos distintos · pp. 17-19**

La aplicación puede mantener su propia sesión. Deben conocerse y probarse los mecanismos de cierre y revocación de cada contexto pertinente.

**08 · Fronteras diferentes · pp. 20-22**

El widget cambia la presentación; el permiso limita el repositorio. Una copia externa requiere tratamiento propio: no desaparece al retirar el acceso original.

**09 · Solicitante y recurso · pp. 18-25**

Debe demostrarse la autorización de Marta sobre ese documento. La capacidad de la cuenta técnica no basta para justificar la entrega.

**10 · Accesos reintroducidos · pp. 23-25**

Una copia antigua puede recuperar concesiones retiradas. Reconcilia la política actual y repite las pruebas de restricciones y bajas antes de reabrir.

**Señal de comprensión:** puedes cambiar el usuario, el documento o el canal y mantener el razonamiento sin recurrir a «dar control total» ni a «ocultarlo en la pantalla».




GLOSARIO / ACCESO Y MODELO

# Un vocabulario común para revisar permisos

Definiciones de uso en este cuaderno. Los detalles de producto deben contrastarse con la versión y el diseño implantados.

### Identidad / cuenta

Representación con la que un sistema reconoce a una persona o servicio. El nombre visible no sustituye a sus identificadores de correspondencia.

### Autenticación

Verificación de una identidad. Puede utilizar credenciales, factores o información de un proveedor de identidad según el mecanismo configurado.

### Autorización

Decisión sobre si una identidad puede ejecutar una operación concreta sobre un recurso. No queda resuelta solo por haber iniciado sesión.

### ACL / ACE

ACL: lista de control de acceso. ACE: entrada de esa lista. Una entrada aislada no explica necesariamente el acceso efectivo del usuario.

### Permiso efectivo

Resultado de evaluar las condiciones y asignaciones aplicables al acceso. Debe contrastarse con la operación, el recurso y la identidad de la prueba.

### Propietario y grupo propietario

Vías de asignación de acceso sobre un elemento. Deben revisarse junto con el resto de concesiones; el creador técnico también merece atención.

### Public Access

Entrada de acceso del repositorio cuyo alcance debe comprobarse. No equivale por su nombre a un enlace anónimo publicado en Internet.

### Grupo

Conjunto de identidades gestionado con un criterio definido. Su pertenencia necesita gobierno y puede influir en los permisos asignados en otros sistemas.

### Rol del Workspace

Participación local en el expediente a la que se asocian participantes y permisos. No equivale a un privilegio administrativo global.

### Herencia / propagación

La herencia describe el origen de permisos según una regla; la propagación aplica cambios a un alcance. No deben presumirse como sincronización universal continua.

**Uso del vocabulario:** elige la palabra por la responsabilidad que describe. «Rol», «grupo», «sesión» y «permiso» no son sinónimos ni sustituyen una prueba del recurso.

[1] [2] [4] [5] [7] [8] [9] [10] [11] [12] [14] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




GLOSARIO / IDENTIDAD Y OPERACIÓN

# Entender el recorrido sin mezclar conceptos

Definiciones de uso en este cuaderno. Los detalles de producto deben contrastarse con la versión y el diseño implantados.

### Partición y recurso OTDS

La partición organiza identidades; el recurso representa una aplicación integrada. El estado correcto en una no demuestra por sí solo el del otro.

### Aprovisionamiento

Creación o mantenimiento de cuentas y grupos en un destino. Es distinto de autenticar una sesión y de autorizar la lectura del certificado.

### IdP / federación

IdP es el proveedor de identidad. La federación permite confiar en información de autenticación entre componentes conforme a un mecanismo validado.

### SSO / MFA

SSO: inicio de sesión único. MFA: autenticación con varios factores. Ambos tratan la identidad, sin eliminar la autorización propia de cada recurso.

### SAML / OpenID Connect

Mecanismos de federación que pueden intervenir en una arquitectura de identidad. Su uso concreto exige compatibilidad y configuración de los componentes implicados.

### Ticket, token y cookie de sesión

Elementos que pueden transportar o mantener contexto de acceso. Se interpretan según su emisor y consumidor; no son contraseñas ni equivalentes entre sí.

### Cuenta de servicio

Identidad utilizada por una integración o proceso. Debe tener responsable, alcance y control de credenciales; no sustituye la autorización del solicitante.

### Mínimo privilegio

Asignar solo las capacidades necesarias para la tarea y el recurso. El alcance se revisa cuando cambian la función o la necesidad de negocio.

### Trazabilidad / auditoría

Información que permite atribuir y reconstruir actuaciones. Debe registrar el contexto necesario, protegerse y evitar secretos o datos no pertinentes.

### Revocación efectiva

Retirada demostrada de la capacidad de acceso pertinente. Puede exigir actuar sobre asignaciones y sesiones; una solicitud de baja no equivale al cierre.

**Uso del vocabulario:** elige la palabra por la responsabilidad que describe. «Rol», «grupo», «sesión» y «permiso» no son sinónimos ni sustituyen una prueba del recurso.

[1] [2] [4] [5] [7] [8] [9] [10] [11] [12] [14] Bases conceptuales. Modelos y ejercicios originales del caso; referencias en pp. 36-37.




GUÍA DEL FORMADOR / CONDUCCIÓN DE LA SESIÓN

# Enseñar a justificar y comprobar una restricción

Duración orientativa: 6 horas, incluidas pausas. Puede impartirse en dos sesiones sin acceso a un entorno real.

| Tiempo | Trabajo propuesto |
|---|---|
| 20 min | Recuperar la matriz del módulo 3 y acordar el objetivo. |
| 75 min | Fichas 26-28: permisos, identidades, ACL y herencia. |
| 15 min | Pausa. |
| 50 min | Fichas 29-30: OTDS, directorio, SSO y sesiones. |
| 50 min | Fichas 31-32: Workspace, integración y controles. |
| 15 min | Pausa. |
| 65 min | Caso integrador: 35 minutos de trabajo y 30 de debate. |
| 30 min | Evaluación individual y autocorrección explicada. |
| 20 min | Completar la ficha de verificación de la página 35. |
| 20 min | Repasar errores y reconstruir una retirada completa. |

## Durante cada ficha

Pide al alumno que identifique usuario, recurso y operación. Cambia una variable: otra cuenta, un documento nuevo o una sesión anterior. Comprueba si mantiene la regla sin ampliar accesos por comodidad.

## Errores que conviene detener

«SSO concede acceso a todo»; «sin una fila individual nadie entra»; «corregir la plantilla arregla lo anterior»; «baja en AD significa cierre instantáneo». Pide siempre qué evidencia permitiría sostener cada afirmación.

## Cierre observable

Cada participante debe explicar una concesión, una restricción y una retirada. Después debe proponer una prueba permitida y otra no permitida usando identidades ordinarias y contenido ficticio.

**Laboratorio opcional:** usar cuentas y documentos de prueba, cambios autorizados y un plan de reversión. No ensayar revocaciones, fallos de confianza ni modificaciones masivas sobre usuarios reales.




HERRAMIENTA DE TRABAJO / FICHA REUTILIZABLE

# Verificación de un cambio de acceso

Utiliza una copia por cambio o revisión. Cada resultado debe apuntar a una evidencia, no a una impresión del revisor.

**Expediente / nodo:** _____ **Entorno:** _____

**Cambio / solicitud:** _____ **Responsable:** _____ **Fecha:** _____

| Punto de control | Evidencia o referencia registrada | Resultado |
|---|---|---|
| Identidad real, recurso y operaciones autorizadas. | | C / NC / NA |
| Grupos, roles, propietario y otras concesiones. | | C / NC / NA |
| Operaciones permitidas y excluidas por los canales previstos. | | C / NC / NA |
| Contenido anterior, altas nuevas y excepciones. | | C / NC / NA |
| Cambio de función, retirada y sesiones pertinentes. | | C / NC / NA |
| Integración, credenciales, auditoría y recuperación. | | C / NC / NA |

**C:** cumple. **NC:** no cumple. **NA:** no aplica; justificarlo. Registrar aparte los pendientes y la persona que debe resolverlos.

**Decisión y validación:** _____
**Pendientes / siguiente revisión:** _____




REFERENCIAS / PRODUCTO Y AUTORIZACIÓN

# Fuentes para profundizar

Consulta documental: 23 de septiembre de 2026. Los títulos son enlaces activos; la numeración coincide con el pie de las fichas.

### [1] OpenText · Content Server REST API, 26.1

Catálogo de operaciones sobre permisos de nodo, propietario, grupo, acceso público y permisos efectivos. Referencia técnica de esa versión; no se declara como versión instalada.

### [2] OpenText · pyxecm: Content Server

Documentación del proyecto publicado por OpenText: permisos, destinatarios, alcance sobre descendientes y operaciones de roles. No sustituye a las guías de administración.

### [3] OpenText · Permissions Explorer

Descripción oficial de comparación y cambio de permisos mediante Permissions Explorer. Referencia conceptual para revisar accesos, no garantía de una interfaz idéntica en todas las versiones.

### [4] OpenText · OTDS: curso 3-0300

Programa oficial: sincronización, autenticación, particiones, recursos, roles de acceso e integración con Content Management. Su alcance formativo no prueba una configuración concreta.

### [5] OpenText · pyxecm: Directory Services

Referencia de objetos y operaciones OTDS, incluidas particiones sincronizadas, recursos y manejadores de autenticación. Ayuda a distinguir responsabilidades; no garantiza latencias de sincronización.

### [6] OpenText · Permisos de una plantilla xECM

Material oficial sobre participantes, grupos y roles de equipo en plantillas. Corresponde a Extended ECM 16.2; no se utiliza para prescribir pantallas ni comportamientos universales.

### [7] OWASP · Authorization Cheat Sheet

Principios de mínimo privilegio, autorización por solicitud y control en el lado servidor. Base de las pruebas permitidas y excluidas del caso; no describe la semántica de una ACL OpenText.

**Lectura de las fuentes:** los conceptos documentados se distinguen de las decisiones, cifras, modelos y soluciones ficticias desarrolladas para Bahía Ingeniería.




# Contrastar conceptos antes de implantar

Consulta documental: 23 de septiembre de 2026. Los títulos son enlaces activos; la numeración coincide con el pie de las fichas.

### [8] OpenID Foundation · How Connect Works

Explicación primaria de OpenID Connect y de la función del ID token. Se utiliza para distinguir autenticación y acceso a recursos, no para afirmar compatibilidad de cualquier versión OTDS.

### [9] Microsoft · Revocar acceso de un usuario

Documentación de Microsoft Entra sobre tokens y sesiones de aplicación. Ilustra por qué la retirada requiere conocer cada contexto; no se trasladan sus comandos a Content Server.

### [10] OWASP · Session Management

Principios de gestión, terminación y protección de sesiones. Base conceptual para diferenciar sesiones antiguas, nuevos accesos y cierre; no fija plazos de producto.

### [11] OWASP · Logging Cheat Sheet

Diseño y protección de registros de seguridad, contexto del evento y datos que no deben registrarse. Se aplica al diseño de evidencias del cuaderno.

### [12] OWASP · Secrets Management

Gobierno del ciclo de vida de secretos: almacenamiento, acceso, rotación y revocación. Referencia general para cuentas e integraciones, no un procedimiento concreto de OpenText.

### [13] OWASP · REST Security

Controles de comunicaciones, autenticación y autorización de APIs. Se utiliza para delimitar la responsabilidad de las integraciones que entregan contenido al usuario.

### [14] OWASP · Multifactor Authentication

Definición y tratamiento de múltiples factores de autenticación. Base para distinguir MFA de SSO y de los permisos documentales; no se promete una cobertura automática.

**Antes de configurar:** confirmar versión, licencias, integración y reglas de acceso; consultar la ayuda aplicable; probar altas, cambios, bajas y restauraciones. Este cuaderno no sustituye esa validación.