Modelo de permisos de OpenText

Entender qué puede hacer cada usuario sobre cada elemento

OpenText controla el acceso mediante permisos aplicados a usuarios y grupos sobre nodos del repositorio. La combinación de permisos determina si una persona puede ver, abrir, modificar, añadir contenido, reservar o eliminar elementos.

01

ACCESO

Los permisos establecen las operaciones autorizadas sobre documentos, carpetas y otros objetos del repositorio.

02

GRANULARIDAD

No todo acceso implica modificación: visualizar, añadir, editar o eliminar son capacidades diferenciadas.

03

CONTEXTO

El permiso efectivo depende del usuario, sus grupos, la ACL del objeto y la herencia existente.

IDEA CLAVE

Acceder no significa poder hacerlo todo.

El modelo separa capacidades para aplicar el principio de mínimo privilegio y adaptar la seguridad a cada contexto documental.

IDENTIDAD | ACL | PERMISOS | OPERACIÓN | RESULTADO

Usuarios, grupos y roles

Tres conceptos distintos para expresar identidad y responsabilidad

Los usuarios representan identidades concretas; los grupos reúnen identidades con características comunes; los roles expresan una función dentro de un contexto, especialmente en Business Workspaces. Combinarlos correctamente simplifica la administración.

01

USUARIO

Identidad individual autenticada que accede a OpenText y realiza acciones trazables.

02

GRUPO

Conjunto administrable de usuarios al que pueden asignarse permisos comunes.

03

ROL

Función contextual -por ejemplo responsable o colaborador- que puede ser ocupada por usuarios o grupos.

IDEA CLAVE

Identidad, pertenencia y función no son lo mismo.

Usar grupos para pertenencia y roles para responsabilidad evita construir modelos de seguridad basados en excepciones personales.

USUARIO	GRUPO	ROL	PERMISOS	CONTENIDO

ACL y herencia de permisos

Cómo se construye el acceso efectivo en el repositorio

La Access Control List (ACL) identifica quién tiene acceso a un objeto y con qué permisos. En estructuras jerárquicas, la herencia permite transmitir seguridad desde niveles superiores, aunque el diseño debe controlar cuidadosamente las excepciones.

01

ACL

Relaciona usuarios o grupos con el conjunto de permisos aplicable sobre un objeto.

02

HERENCIA

Permite que una estructura reciba permisos desde su contexto superior y mantenga un comportamiento coherente.

03

EXCEPCIONES

Cambiar permisos localmente puede ser necesario, pero multiplica la complejidad si se convierte en la regla.

IDEA CLAVE

La seguridad sencilla es más fácil de gobernar.

Conviene diseñar patrones heredables y limitar las excepciones. Cuantas más ACL únicas existan, más difícil resulta entender y mantener el acceso.

NIVEL SUPERIOR → HERENCIA → ACL LOCAL → PERMISO EFECTIVO → ACCESO

OTDS + Active Directory

Identidad corporativa conectada con los servicios OpenText

OpenText Directory Services (OTDS) puede integrar identidades procedentes de directorios corporativos como Active Directory y proporcionar una capa común de autenticación y gestión de recursos para las aplicaciones OpenText.

01

DIRECTORIO

Active Directory mantiene las identidades y grupos corporativos que la organización utiliza como referencia.

02

OTDS

Sincroniza o relaciona identidades y las presenta de forma utilizable por los recursos OpenText.

03

APLICACIONES

Content Management y otros servicios OpenText consumen esa identidad para autenticar y autorizar usuarios.

ACTIVE DIRECTORY | **OTDS** | **IDENTIDAD** | **RECURSO OT** | **ACCESO**

IDEA CLAVE

La identidad debe tener una fuente clara.

OTDS no sustituye el diseño de permisos de Content Management: resuelve identidad y autenticación; el repositorio sigue gobernando qué puede hacer cada identidad.

Single Sign-On (SSO)

Una autenticación corporativa para acceder a los servicios autorizados

El Single Sign-On evita solicitar credenciales repetidamente cuando existe una sesión corporativa válida. La identidad se autentica mediante el mecanismo previsto y los servicios confían en la información de autenticación intercambiada.

01

AUTENTICACIÓN

El usuario demuestra su identidad ante el proveedor o mecanismo corporativo configurado.

02

CONFIANZA

Los componentes participantes intercambian o validan la información necesaria para reconocer esa identidad.

03

AUTORIZACIÓN

Una vez identificado el usuario, cada aplicación aplica sus propios permisos y reglas de acceso.

IDEA CLAVE

SSO autentica; no concede permisos por sí mismo.

Una sesión válida permite saber quién es el usuario. Después, Content Management decide a qué contenido puede acceder y qué acciones puede realizar.

USUARIO	AUTENTICACIÓN	SSO	OPENTEXT	AUTORIZACIÓN

Seguridad aplicada a Workspaces

Convertir responsabilidades de negocio en acceso documental

En xECM, la seguridad de un Business Workspace puede apoyarse en roles y participantes vinculados al objeto de negocio. Esto permite que el acceso acompañe al contexto y no dependa de administrar manualmente cada documento.

01

PARTICIPANTES

Las personas o grupos relacionados con el objeto de negocio se incorporan al contexto del Workspace.

02

ROLES

Cada función puede asociarse a capacidades y responsabilidades coherentes dentro del espacio.

03

PROPAGACIÓN

La estructura y los documentos pueden recibir la seguridad prevista por el modelo del Workspace.

IDEA CLAVE

La seguridad debe seguir al negocio.

Cuando cambian responsables o participantes, el modelo debe permitir actualizar el acceso sin reconstruir manualmente la seguridad de todo el expediente.

OBJETO | PARTICIPANTES | ROLES | WORKSPACE | **DOCUMENTOS**

Buenas prácticas de seguridad xECM

Diseñar un modelo comprensible, mantenible y verificable

La seguridad xECM debe partir de reglas de negocio claras y traducirse a grupos, roles, ACL y herencia. El objetivo no es crear el mayor número posible de restricciones, sino un modelo que pueda explicarse, auditarse y mantenerse.

01

MÍNIMO PRIVILEGIO

Conceder únicamente las capacidades necesarias para la función y el contexto de cada participante.

02

PATRONES

Preferir grupos, roles y herencia frente a permisos individuales y excepciones repetidas.

03

VALIDACIÓN

Probar el acceso con perfiles reales y revisar periódicamente cambios, grupos, roles y excepciones.

IDEA CLAVE

Si no puede explicarse, será difícil administrarlo.

Un buen modelo de seguridad debe permitir responder con claridad quién accede, por qué accede, qué puede hacer y de dónde procede ese permiso.

REQUISITO | MODELO | CONFIGURACIÓN | PRUEBA | REVISIÓN