
Cómo operar un centro de experiencias de forma segura

Por qué un museo, un centro de ciencia o un centro de experiencia de marca debe gestionarse como un parque informático bien gobernado, y cómo lo consigue taleor: cada dispositivo identificado, cada conexión cifrada, cada cambio atribuido, cada visitante anónimo.

Documento técnico · octubre de 2026 · Versión 1.0

Para directores, responsables técnicos y de TI, integradores audiovisuales, consultores y comités de licitación de museos, centros de ciencia, centros de experiencia de marca, sitios patrimoniales y atracciones.

taleor

Índice

1	Resumen ejecutivo	3
2	El problema: un espacio es hoy un parque informático	3
3	Lo que un espacio necesita realmente	5
4	Cómo funciona taleor	6
5	Seguro desde el diseño	8
6	Configurado por un asistente	13
7	Análisis: lo que aprende un espacio	14
8	Funciona en cualquier plataforma, con lo que ya tiene	15
9	Modelos de implantación y cómo evaluarlos	17
10	Acerca de taleor	19
	Fuentes y verificación	19

1 Resumen ejecutivo

Un espacio de experiencias solía ser un edificio con algunas pantallas. Hoy es una red: cientos de equipos, pantallas, proyectores, altavoces, luminarias y sensores de una docena de fabricantes, cada uno con su propio firmware, una dirección y, a menudo, una contraseña, gestionados por un equipo pequeño que no es un equipo de TI.

Este documento sostiene que un espacio debe gestionarse como se gestiona un parque informático bien administrado: cada dispositivo identificado, cada conexión cifrada, cada cambio atribuido, cada actualización verificada, cada visitante anónimo. La sección 3 expone siete principios, las secciones 4 a 8 describen cómo los cumple taleor y la sección 9 concluye con una lista de comprobación que un comité de licitación puede plantear a cualquier proveedor, incluidos nosotros.

Con taleor, usted gestiona un espacio de experiencias de forma segura y agéntica: su contenido, sus aplicaciones interactivas, sus pantallas y su hardware, desde una sola consola. Se apoya en tres pilares: es seguro desde el diseño; lo configura un asistente que nunca aplica un cambio sin la aprobación de una persona identificada por su nombre; y sus análisis indican «sin medir» en lugar de cero. Funciona como aplicación web, como aplicación de escritorio para Windows, macOS y Linux, y como servidor local en su propio edificio, incluso totalmente aislado de la red (air gap). Sus pantallas funcionan con Windows, macOS, Linux, Raspberry Pi y Android. Controla equipamiento de cualquier marca mediante estándares abiertos.

2 El problema: un espacio es hoy un parque informático

2.1 Cientos de dispositivos, decenas de marcas, un equipo pequeño

Cuente los equipos que hay en las salas de un museo actual: uno detrás de la mayoría de los módulos, además de pantallas en red, proyectores, procesadores de audio, controladores de iluminación, sensores, lectores y pulsadores. En un espacio de tamaño modesto, la cifra alcanza unos pocos cientos. Los datos de ejemplo utilizados para desarrollar taleor, basados en un museo regional típico, contienen 69 módulos y 342 dispositivos que utilizan 49 protocolos de control. Es un parque corriente.

Cada fabricante aporta su propio protocolo, su propia herramienta de gestión y su propia idea de cómo funcionan las actualizaciones. El contenido cambia cada temporada. El equipo suele estar formado por entre dos y cinco personas cuyos

puestos no se concibieron para gestionar una flota de dispositivos ni aplicar parches.

2.2 Exposición a riesgos de seguridad

Cuatro puntos débiles se agravan entre sí.

Credenciales predeterminadas. El equipamiento audiovisual profesional se entrega con una interfaz de gestión y una contraseña de fábrica que rara vez se cambia, porque cambiarla en doscientos dispositivos supone una semana de trabajo que no es responsabilidad de nadie. La botnet Mirai de 2016 captaba dispositivos probando una lista corta de contraseñas de fábrica. El equipamiento audiovisual de los espacios no es una excepción.

Pantallas sin parches. El equipo situado detrás de un módulo suele seguir ejecutando el sistema operativo con el que se puso en marcha, porque actualizarlo implica cerrar el módulo. Un equipo sin parches en la misma red que la venta de entradas y la gestión técnica del edificio es una vía de entrada. Los marcos con los que se evalúa a los organismos públicos de Alemania, los Países Bajos y Polonia (BSI IT-Grundschutz, la Baseline Informatiebeveiliging Overheid y las obligaciones derivadas de NIS2) consideran la aplicación oportuna de parches y el inventario de activos como controles básicos.

Secretos compartidos. Muchos sistemas de control autentican una pantalla con una clave guardada en un archivo de configuración. Cualquiera que pueda leer ese archivo puede hacerse pasar por la pantalla.

Dependencia de la nube. Un sistema que se detiene cuando falla internet o la nube del proveedor ha trasladado el punto único de fallo a un lugar que el espacio no puede reparar. Para una institución pública es también una cuestión de contratación: ¿quién custodia los datos, bajo qué legislación y qué ocurre cuando termina el contrato?

2.3 Interrupciones, puntos ciegos y dependencia del proveedor

Las interrupciones son el fallo más visible y el menos medido. Una pantalla se congela a las 10:00, un visitante lo comenta al mediodía, el técnico se entera a las 14:00 y nada ha registrado las cuatro horas perdidas.

La mayoría de los espacios cuentan a los visitantes en la entrada y en ningún otro lugar. No pueden decir en qué módulo se detuvo la gente, durante cuánto tiempo ni si un vídeo se vio hasta el final. Donde existe medición, suele ser un sistema independiente y, con demasiada frecuencia, uno con cámaras que identifican a las personas.

Cada subsistema llega con su propio proveedor y su propio contrato. Cuando un proveedor es adquirido o abandona un producto, el contenido creado para un sistema de reproducción propietario no puede trasladarse, y el hardware que solo se comunica con un controlador concreto se convierte en chatarra. La pregunta que debe plantearse un comité no es «¿este proveedor es compatible con nuestro hardware?», sino «si este proveedor desapareciera, ¿qué seguiría siendo nuestro?».

3 Lo que un espacio necesita realmente

Estos problemas ya se han resuelto antes, en la informática de uso general. Lo que faltaba era aplicar esas soluciones a la realidad de un espacio de experiencias: muchos equipos pequeños, muchas marcas, un equipo reducido, un público general y un edificio que tiene que abrir a las 10:00. Proponemos siete principios.

1. **Cada dispositivo tiene una identidad que no se puede copiar.** Una clave generada en su propio hardware que nunca ha salido de él. No una contraseña. No un token en un archivo.
2. **Cada conexión está cifrada y autenticada en ambos sentidos.** Con menos que eso, un extraño en la red del espacio puede montar una imitación convincente.
3. **En una pantalla no se ejecuta nada que no se haya verificado antes.** Los controladores y las actualizaciones se comprueban mediante una firma o una suma de comprobación en la propia pantalla, no solo en el origen.
4. **Cada cambio tiene un nombre y una hora.** Un registro de auditoría que un administrador puede reducir a un día, o editar, no es un registro de auditoría.
5. **Las personas reciben los permisos que su trabajo requiere, y ninguno más.** Un responsable de instalaciones puede reiniciar una pantalla congelada sin poder eliminarla.
6. **Los visitantes permanecen anónimos por diseño, no por política.** Una propiedad del esquema de la base de datos, y comprobada mediante pruebas.
7. **El sistema pertenece al espacio.** Puede ejecutarlo todo en su propio edificio, sin internet, y puede cambiar de proveedor sin perder su contenido.

Esto es lo que cualquier departamento de TI competente exigiría a una flota de doscientos equipos. El resto de este documento describe cómo los cumple taleor.

4 Cómo funciona taleor

4.1 Los componentes

La consola. Una aplicación web en la que el personal ve cada módulo, cada pantalla y cada elemento del equipamiento, carga contenido, define programaciones y disparadores, supervisa el estado y las alertas y consulta los análisis. Funciona en cualquier navegador actual o como aplicación de escritorio para Windows, macOS y Linux.

El agente de pantalla. Un pequeño servicio en segundo plano en el equipo situado detrás de cada módulo. Mantiene una conexión persistente y mutuamente autenticada con el servidor, reproduce lo que se le indica, controla el equipamiento conectado a ese equipo, lee sus sensores, informa de su estado y se mantiene actualizado. De forma predeterminada guarda una copia local de 4 GB de su contenido y sigue reproduciendo cuando el servidor no está disponible. Los agentes funcionan con Windows, macOS, Linux, Raspberry Pi y Android. Una pantalla sin equipo se vincula como pantalla en navegador mediante un código de seis dígitos que se lee en la propia pantalla.

Controladores. Un paquete firmado que indica a taleor qué puede hacer un elemento del equipamiento y cómo comunicarse con él. La consola solicita una acción, como alimentación, fuente o volumen; el controlador se encarga del protocolo.

El servidor. La base de datos, los hubs WebSocket que transmiten el estado en vivo, la autoridad de certificación de cada espacio, el almacenamiento multimedia, el motor de programación, el monitor de alertas, el registro de auditoría y los análisis. Es el mismo software en nuestra nube o en una máquina de su edificio, con o sin internet.

4.2 Una compilación, tres formas de ejecutarla

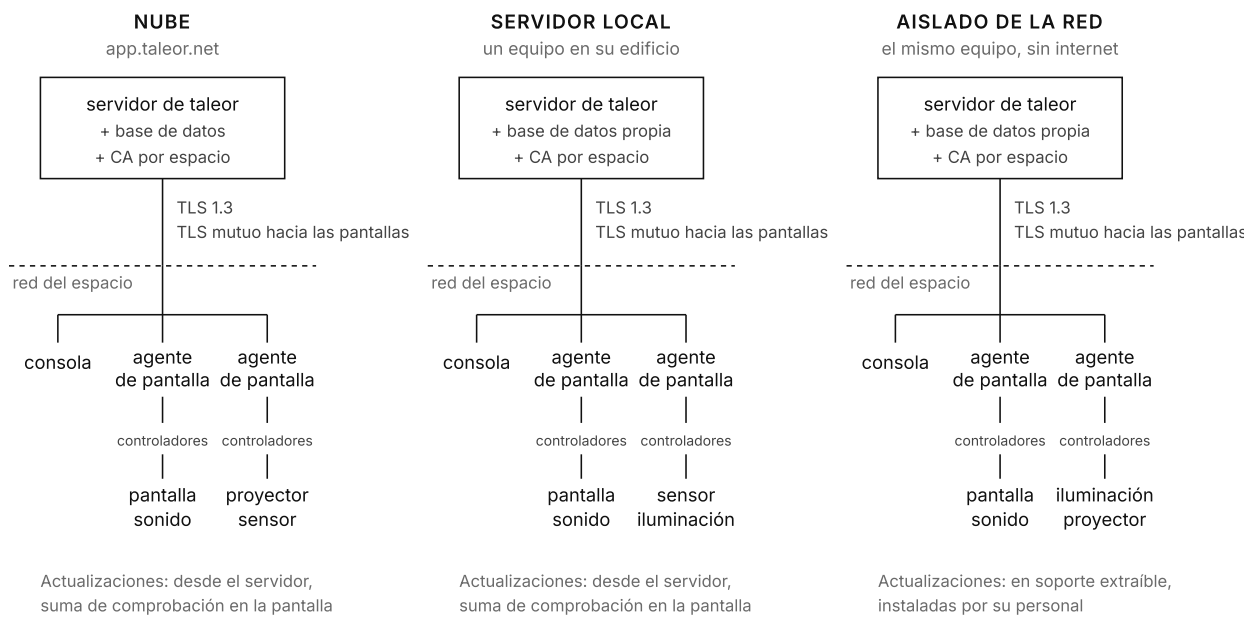


Figura 1. Una compilación, tres formas de ejecutarla. El mismo servidor, la misma consola y los mismos agentes de pantalla en la nube, en un servidor local en el edificio o aislados de la red, sin internet.

En el modo en la nube, la consola y el servidor se encuentran en app.taleor.net y son los agentes quienes inician la conexión hacia ellos; el equipamiento de la red del espacio lo controlan los agentes situados dentro de esa red. En el modo de servidor local, el mismo paquete se instala en una máquina Windows, macOS o Linux del edificio, con su propia base de datos privada y su propia autoridad de certificación, de modo que la consola, las pantallas, el contenido multimedia y el registro de auditoría permanecen dentro. En el modo aislado de la red, ese servidor funciona sin ninguna conexión a internet: el entorno de ejecución y la base de datos vienen incluidos en el paquete, no se descarga nada durante la instalación y su propio personal introduce las actualizaciones en soportes extraíbles. Un único código base, una única consola; un espacio que empieza en la nube puede pasar a sus propias instalaciones.

5 Seguro desde el diseño

5.1 Identidad: una clave que nunca sale de la máquina

taleor sustituye el secreto compartido por un certificado. Cuando se registra una pantalla, esta genera un par de claves asimétricas en su propia máquina y envía solo la mitad pública, en una solicitud de firma de certificado, a la autoridad de certificación del espacio, que firma y devuelve un certificado. La clave privada nunca se transmite. A partir de ese momento, la pantalla demuestra su identidad generando una firma, en tiempo real, durante cada negociación TLS. No hay nada que copiar.

Una autoridad de certificación por espacio, que un administrador abre desde la consola. Si un espacio se ve comprometido, no se puede generar con ello una identidad en otro. La clave privada de la autoridad se guarda cifrada con un secreto independiente de los demás secretos del servidor.

No se confía en la solicitud. De la solicitud de firma solo se toma la clave pública; el sujeto, el periodo de validez y todas las extensiones los fija el servidor, de modo que una pantalla no puede pedir que se la llame con el nombre de otra pantalla ni convertirse en autoridad de certificación. Los certificados de pantalla se emiten solo para la autenticación de clientes, por lo que uno robado no puede servir para montar un servidor falso.

No existe un botón «Emitir certificado». Un certificado cuya clave privada hubiera estado alguna vez en poder del servidor anularía el propósito.

5.2 Transporte: cifrado y comprobado, en ambos sentidos

Toda conexión entre un navegador, una pantalla y la consola se transmite mediante TLS 1.3 (se acepta 1.2 para clientes más antiguos). Las conexiones de las pantallas utilizan TLS mutuo: cada parte presenta su certificado a la otra.

Un certificado válido es necesario, pero no suficiente. En cada conexión, el servidor comprueba además, contra la base de datos y no contra una lista en caché, que el certificado no esté revocado ni caducado, que el dispositivo que nombra siga existiendo y que ese dispositivo pertenezca al espacio para el que se emitió el certificado.

Los certificados duran 398 días, el límite máximo del CA/Browser Forum para certificados de confianza pública, y se renuevan durante sus últimos 30 días a través de la propia conexión de TLS mutuo de la pantalla, de modo que una flota renueva sus credenciales sin necesidad de visitas in situ. La emisión de un certificado nuevo revoca el anterior.

La activación del TLS mutuo es progresiva: un modo de transición acepta tanto un certificado como la credencial anterior mientras la flota se migra sala por sala, y después un modo obligatorio cuando todos los puntos de conexión tienen certificado. El servidor rechaza ese cambio mientras algún dispositivo que se conecte pudiera quedar bloqueado, porque la alternativa es un museo a oscuras. Si se vuelve a desactivar el modo, el cambio se revierte de inmediato.

5.3 Integridad: no se ejecuta nada que no se haya verificado

Los controladores están firmados. Un controlador es un paquete con un manifiesto y una firma Ed25519 separada sobre el resumen criptográfico del paquete. Un servidor de producción rechaza de forma predeterminada un paquete sin firmar, porque un controlador es código que abre sockets y se comunica con el hardware. Los integradores y fabricantes pueden escribir y firmar los suyos con el kit de controladores.

Las actualizaciones de las pantallas se verifican mediante una suma de comprobación. El servidor publica una versión con su suma de comprobación SHA-256. La pantalla verifica la suma antes de cualquier otra cosa, extrae la actualización en un directorio de preparación, la pone en lugar de la versión actual y se reinicia. Una verificación fallida supone una actualización rechazada.

Las actualizaciones respetan el edificio. Una actualización solo se instala fuera del horario de apertura. Una versión nueva que no supera su comprobación de estado en diez minutos se revierte y se bloquea para que no vuelva a intentarse. Un espacio puede excluir una pantalla de las actualizaciones; una pantalla excluida o rezagada aparece marcada como «No actualizado» en la consola, de modo que nunca queda olvidada sin que nadie lo advierta.

5.4 Acceso y roles

taleor tiene cinco roles asignables.

Rol	Para qué sirve
Administrador de red	Todo, en todos los espacios que gestiona la organización
Administrador de conjunto	Todos los permisos de alcance de espacio, en los espacios de un conjunto
Administrador de espacio	Todos los permisos de alcance de espacio, en un espacio
Gestor de contenidos	Contenido, reels, programaciones y plantillas
Responsable de instalaciones	Manejo del equipamiento: reiniciar, alimentación, fuente, volumen

Los roles son deliberadamente generales, porque un modelo de permisos que nadie sabe explicar es un modelo que nadie aplica. Cada ruta comprueba tanto el rol como el espacio, de modo que una persona con derechos en un espacio no ve nada de otro. El inicio de sesión es individual y nunca se comparte; una cuenta nueva debe cambiar su contraseña en el primer uso.

5.5 El registro de auditoría

Cada operación de escritura queda en el registro de auditoría con la persona, la acción, la hora y la dirección de red de la que procede. Esto incluye las acciones realizadas por el asistente, que se registran como aplicadas por el asistente en nombre de una persona identificada. El registro se puede filtrar en la consola y exportar como CSV con los mismos filtros, para que un auditor pueda llevárselo.

Dos propiedades protegen el registro frente a las personas con más poder sobre él. La categoría de auditoría tiene un periodo mínimo de conservación obligatorio de 180 días: un espacio puede conservar su registro durante más tiempo, nunca menos. Y cuando un miembro del personal ejerce su derecho de supresión, la cuenta se convierte en una lápida (tombstone): identidad ocultada, direcciones de red eliminadas, acciones conservadas, de modo que el registro sigue indicando que alguien, cuyos datos se suprimieron después, publicó una escena el día tres. Un administrador no puede suprimir su propia cuenta.

5.6 Privacidad de los visitantes, por diseño

Los visitantes de un espacio son público general, muchos de ellos niños. El diseño correcto es aquel en el que el sistema no puede registrar quiénes son.

Las dos tablas que contienen el comportamiento de los visitantes, eventos de presencia y eventos de interacción, guardan un espacio, un dispositivo, una zona, una palabra de estado o de evento y una marca de tiempo. No contienen ningún identificador de la persona: ni dirección de red, ni rostro, ni cookie, ni sesión. Es una propiedad del esquema, no una promesa en una política; una prueba lo verifica contra las definiciones reales de las tablas y hace fallar la compilación si alguien añade una columna de ese tipo.

Detrás hay un registro de actividades de tratamiento que reside en el código y se revisa en el mismo cambio que el código que genera los datos: finalidad, base jurídica, grado de identificación, destinatarios y plazo de conservación de cada categoría. Una limpieza nocturna elimina las filas cuyo plazo de conservación ha vencido, por bloques para no ralentizar nunca un espacio abierto, y escribe una fila por cada ejecución, incluidos los fallos. Ese registro es la prueba que un auditor solicita en primer lugar.

Categoría de datos	Conservación predeterminada	Mínimo
Presencia en un módulo	400 días	1 día
Toques y elecciones	400 días	1 día
Qué se reprodujo, y cuándo	1825 días	365 días
Registros de las pantallas	30 días	1 día
Quién hizo qué (auditoría)	730 días	180 días

Los controles se han desarrollado según los requisitos técnicos de ISO/IEC 27701, la extensión de privacidad de ISO/IEC 27001. Somos prudentes con esta afirmación: un producto no puede certificarse conforme a 27701; una organización sí, tras una auditoría. taleor implementa los controles técnicos de la norma y genera las pruebas que necesita un auditor; la institución sigue teniendo que designar a un responsable de privacidad, realizar su evaluación de impacto, formalizar sus contratos de encargo del tratamiento y colocar avisos en las salas.

5.7 Emergencia

Un único control activa un aviso de emergencia en todo el espacio, en una planta, en una zona o en las pantallas elegidas. El mensaje ocupa toda la pantalla, un aviso se desplaza por la parte inferior y el sonido de los módulos se silencia. Una pantalla que se reconecta durante una difusión también la recibe. El aviso puede

iniciarse y finalizarse desde un dispositivo portátil del personal, y queda auditado como cualquier otra acción. Decimos «sonido de los módulos» deliberadamente: taleor silencia lo que controla, y no es un sistema de megafonía.

5.8 Aislamiento y air gap

El paquete del servidor local instala su propio clúster privado de PostgreSQL, que escucha únicamente en la interfaz de bucle invertido (loopback) y en un puerto no estándar, de modo que nunca entra en conflicto con una base de datos que ya exista en la máquina. Nadie escribe la contraseña de la base de datos: se genera una aleatoria durante la instalación, que solo figura en un archivo de configuración legible por el sistema y sus administradores. No se necesita ningún entorno de ejecución de contenedores. El modo aislado de la red es el mismo paquete sin internet (sección 4.2).

El equipamiento de la red del espacio se controla siempre desde dentro de esa red, mediante los agentes de pantalla o el servidor local. La consola en la nube nunca necesita una ruta hacia el interior de su edificio; los agentes se conectan hacia fuera.

5.9 Modos de fallo seguros

- Una pantalla que pierde el contacto con el servidor sigue reproduciendo su última configuración válida desde su caché local, también tras reinicios, hasta que el servidor vuelve.
- Una pantalla que se desconecta genera una alerta que indica cuál es, dónde está, qué debería estar mostrando y desde cuándo. La alerta se resuelve sola cuando la pantalla vuelve; un fallo repetido actualiza la alerta existente.
- El servidor hace copias de seguridad de su base de datos según una programación, con un historial continuo y restauración desde cualquier punto. Todo lo que se elimina de la biblioteca multimedia se puede recuperar durante 30 días.
- El servidor se niega a imponer el TLS mutuo obligatorio en un espacio mientras algún dispositivo pudiera quedar fuera, rechaza un plan obsoleto del asistente y rechaza un controlador sin firmar. Entre adivinar y detenerse, taleor se detiene y explica por qué.

5.10 Cómo comprobamos nuestro propio trabajo

Antes del lanzamiento, la consola, el software de las pantallas y el sitio web de taleor se sometieron a una revisión de seguridad de aplicaciones: un modelo de amenazas por escrito, exploits de prueba de concepto para cada debilidad

sospechada, escáneres de dependencias y de análisis estático, y un nuevo escaneo tras las correcciones. Cada hallazgo tiene una gravedad, un responsable y una corrección verificada; no se supera una fase mientras haya abierto un hallazgo bloqueante. Exija lo mismo a cualquier proveedor.

6 Configurado por un asistente

6.1 Qué hace

Configurar un módulo interactivo siempre ha sido un trabajo especializado que solo una persona del espacio sabe hacer. taleor incluye en la consola un asistente llamado Oli. Usted escribe lo que quiere:

Cuando alguien se acerque a menos de un metro de la pantalla del vestíbulo, cambiar al vídeo de bienvenida, y volver cuando lleve treinta segundos sin nadie.

El asistente consulta el espacio (módulos, pantallas, reels, entradas declaradas) y propone un plan con la lista exacta de cambios:

Lee pantalla del vestíbulo: sensor de presencia declarado, 2 reels.
Propone: a una distancia de 100 cm o menos, reproducir «vídeo de bienvenida», volver tras 30 s.
A la espera de su revisión.

Usted lo lee. Pulsa «Aplicar» o «Descartar». Cuando falta algo, el asistente dice qué: no hay ningún reel llamado «vídeo de bienvenida», o no hay ningún sensor de presencia en esa pantalla. Si una petición es ambigua, hace una sola pregunta cada vez, y nunca da por supuesto un hardware que no existe.

El asistente propone disparadores, asignaciones de reels y la activación de un disparador, y los aplica una vez que usted los aprueba. Todos los controles siguen disponibles para su uso manual.

6.2 El modelo de permisos

El asistente no es un usuario privilegiado. No tiene permisos propios.

- **Lectura.** Sus herramientas para consultar el espacio son de solo lectura y se limitan al espacio en el que trabaja la persona.
- **Propuesta.** Sus herramientas de planificación solo registran un paso propuesto. No se ejecuta nada. Esto está comprobado mediante pruebas.

- **Aplicación.** Al pulsar «Aplicar», los pasos guardados se ejecutan a través de las mismas funciones de servicio, validaciones y comprobaciones de permisos que si la persona hubiera hecho cada cambio a mano, de modo que una persona que no puede cambiar algo tampoco puede hacer que el asistente lo cambie por ella. El registro de auditoría anota el resultado como aplicado por el asistente en nombre de esa persona identificada.
- **Obsolescencia.** Un plan que ha quedado obsoleto, porque se eliminó un reel entre la propuesta y la aprobación, se rechaza en lugar de completarse por suposición.
- **Contención.** El asistente está desactivado y oculto cuando no está configurado. Su uso se mide, con un límite mensual estricto para todo el servidor. Los errores del servicio subyacente nunca se muestran literalmente.

6.3 Por qué revisar antes de aplicar

Un sistema que cambia lo que se reproduce en doscientas pantallas debe poder responder a «¿quién cambió esto y lo aprobó una persona?». Plantee esa pregunta a cualquier producto que anuncie una configuración automatizada.

7 Análisis: lo que aprende un espacio

7.1 Basados en lo que las pantallas notifican realmente

Los análisis de taleor, llamados «Estadísticas» en la consola, se basan en lo que notifican las pantallas y los sensores, no en un sistema de recuento independiente: el sensor que inicia un vídeo es el mismo que cuenta quién se detuvo y durante cuánto tiempo. Cada cifra se puede acotar a todo el espacio, una planta, una zona o una pantalla, para hoy, esta semana, este mes o este año, con el periodo anterior como comparación.

7.2 Lo que usted ve

Afluencia de visitantes y tiempo de permanencia. Visitantes por hora, día o mes, a partir de sensores y toques. Tiempo de permanencia medio en las visitas con interacción. Las zonas y horas de más afluencia, en un mapa de calor por zona y hora.

Lo que mejor funcionó. Módulos clasificados por visitas y tiempo de permanencia, para que un rincón poco visitado salga a la luz antes de que un conservador pase por delante. Los visitantes y el tiempo de permanencia corresponden al módulo; la disponibilidad y las reproducciones, a cada pantalla.

Prueba de reproducción. Cada elemento, cada reproducción, completa o no, con una exportación CSV que respeta el mismo alcance y periodo. Se conserva cinco años de forma predeterminada, de modo que dura más que la vigencia de una licencia o de un contrato de patrocinio.

Estado y disponibilidad de las pantallas. Disponibilidad de cada pantalla durante el periodo, a partir de los datos de estado. Si no hay datos de estado en un periodo, se muestra como desconocido, no como correcto.

7.3 Cifras honestas

Una cifra que no se puede medir indica «sin medir», nunca cero. Una zona sin sensor no informa de cero visitantes; informa de que allí no se midieron los visitantes.

7.4 Privacidad por diseño, una vez más

Los eventos que hay detrás de cada cifra son los de la sección 5.6, sin ningún identificador del visitante: sin cámaras, sin detección facial, sin seguimiento de dispositivos, sin cookies.

8 Funciona en cualquier plataforma, con lo que ya tiene

8.1 Plataformas

Componente	Funciona en
Consola (aplicación web)	Cualquier navegador actual, en app.taleor.net o en su servidor local
Consola (aplicación de escritorio)	Windows, macOS, Linux
Servidor local, incluido el modo aislado de la red	Windows, macOS, Linux
Agente de pantalla	Windows, macOS, Linux, Raspberry Pi, Android
Pantalla en navegador	Cualquier navegador actual; se vincula con un código de seis dígitos

La aplicación de escritorio abre la consola en su propia ventana, puede reproducir el módulo en el mismo equipo y conserva la última configuración válida tras un reinicio.

8.2 Hardware, mediante estándares abiertos

taleor controla equipamiento de cualquier marca mediante los estándares que ese equipamiento ya utiliza.

Familia	Ejemplos	Mediante
Pantallas	Cualquier pantalla conectada a un equipo que ejecuta el agente de pantalla de taleor, o que muestra la pantalla en navegador	agente de taleor · pantalla en navegador · HDMI
Proyectores	Cualquier proyector compatible con PJLink; protocolos serie específicos de cada fabricante	PJLink · ESC/VP21 · RS-232 · TCP
Sensores	Presencia, distancia (lidar, ultrasonidos), botón sin contacto, pulsador, RFID; controladores de sensores detrás de cualquier pantalla	Serie · USB · TCP
Controladores	OSC de entrada desde una mesa de iluminación o un controlador de espectáculos, OSC de salida desde un disparador, teclas USB, pedales y placas serie, un dispositivo portátil	OSC · USB · serie
Sonido	Procesadores de audio y altavoces en red, desde unos auriculares en un módulo hasta una sala entera	REST · TCP
Iluminación	Iluminación arquitectónica y de módulos	DALI

Lista completa de estándares: PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · serie · USB.

Hay controladores disponibles para estas familias, y los probamos con su equipamiento antes de su apertura; lo dejamos por escrito en lugar de presentar una lista de logotipos. Si un dispositivo no está cubierto, el kit de controladores permite que un integrador escriba uno: un manifiesto, un adaptador, una firma. Los fabricantes pueden traernos un dispositivo y crearemos su integración.

8.3 Qué significa esto para la dependencia del proveedor

La capa de control utiliza estándares abiertos, por lo que el hardware no está ligado a taleor. El servidor funciona en su propia máquina con su propia base de datos, por lo que los datos no están ligados a nuestra nube. El contenido son archivos multimedia corrientes y la configuración se exporta como datos simples, de modo que un espacio que se va se lleva su contenido y su historial. El contenido multimedia también puede permanecer en el Google Drive del propio

espacio: taleor lee solo los archivos seleccionados y las pantallas guardan una copia para la reproducción sin conexión. Preferimos que se quede con nosotros porque el producto es bueno, no porque marcharse sea imposible.

9 Modelos de implantación y cómo evaluarlos

9.1 Tres modelos

Nube. El inicio más rápido: abra app.taleor.net, cree el espacio e instale el agente en el equipo de cada módulo. Los agentes se conectan hacia fuera; nada se conecta hacia dentro. Para espacios sin infraestructura de servidores y para integradores que gestionan varios espacios.

Servidor local. El paquete del servidor en una máquina del edificio, con o sin internet. Para instituciones con su propio departamento de TI y para cualquier espacio cuyas normas de contratación exijan que los datos estén en sus propias instalaciones.

Aislado de la red. El servidor local sin ninguna conexión a internet; el personal introduce las actualizaciones. Para centros con políticas de red estrictas o sin una conectividad fiable, y para quien haya decidido que sus salas no deben depender de una conexión que no controla.

Los tres ejecutan el mismo software y la misma consola, y la elección puede cambiarse más adelante.

9.2 Una lista de comprobación para comités de licitación

Plantee estas preguntas a cualquier proveedor. Nuestras respuestas, con la sección que las respalda:

Pregunta	taleor	Dónde
¿Cómo demuestra cada pantalla su identidad? ¿Interviene una clave o contraseña compartida?	Certificado por pantalla; clave generada en la máquina, nunca copiada; una autoridad por espacio	5.1
¿La conexión de la pantalla está cifrada y autenticada en ambos sentidos? ¿Se pueden renovar los certificados sin visitas in situ?	TLS 1.3; TLS mutuo; certificados de 398 días que se renuevan a través de la propia conexión de la pantalla	5.2
¿Los controladores están firmados? ¿Se verifican las actualizaciones antes de instalarse?	Controladores firmados con Ed25519, los no firmados se rechazan; suma de comprobación SHA-256 verificada en la pantalla	5.3

Pregunta	taleor	Dónde
¿Puede una actualización defectuosa dejar un módulo fuera de servicio?	Se instala fuera del horario de apertura; se revierte y se bloquea si falla la comprobación de estado	5.3
¿Puede un técnico reiniciar una pantalla sin poder eliminarla?	Cinco roles; sí	5.4
¿Cada acción lleva asociada una persona, una hora y una dirección? ¿Puede un administrador reducir o borrar el registro?	Sí; exportación CSV; conservación mínima de 180 días; la supresión deja una lápida, no un hueco	5.5
¿Qué registra el sistema sobre los visitantes y durante cuánto tiempo?	Espacio, dispositivo, zona, estado, hora; ningún identificador, garantizado por una prueba del esquema; conservación por categoría, eliminación documentada	5.6
¿Existe un aviso de emergencia y qué alcance tiene?	Espacio, planta, zona o pantallas elegidas; pantalla completa; sonido de los módulos silenciado	5.7
¿Puede funcionar todo el sistema en sus propias instalaciones, sin internet?	Sí; servidor local y aislado de la red	5.8, 9.1
¿Qué ocurre con los módulos cuando el servidor no está disponible?	Las pantallas siguen reproduciendo desde la caché local, también tras reinicios	5.9
¿Se ha sometido el producto a una revisión de seguridad y podemos ver los hallazgos?	Sí; modelo de amenazas, pruebas de concepto, escáneres, correcciones verificadas	5.10
Si la configuración está automatizada, ¿aprueba una persona cada cambio concreto, en su nombre?	Sí; propuesta, revisión, aplicación; auditado como aplicado en nombre de la persona identificada	6.2
¿Qué plataformas y estándares de hardware?	Pantallas con Windows, macOS, Linux, Raspberry Pi, Android y cualquier navegador; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, serie, USB	8
¿Qué es nuestro si nos vamos?	El contenido como archivos corrientes, la configuración como datos simples, la base de datos en su máquina	8.3

9.3 Qué pedir en un proyecto piloto

Un documento no es un producto. Pida un proyecto piloto con unos pocos módulos que ponga a prueba los controles: registre una pantalla con TLS mutuo e inspeccione su certificado; pruebe una segunda máquina con una copia de su configuración y confirme que se rechaza; pida a un responsable de instalaciones que reinicie una pantalla y que después intente eliminarla; haga que el asistente proponga un disparador, descártelo, apruebe otro y lea el registro de auditoría; desconecte un cable de red y observe cómo la pantalla sigue reproduciendo; exporte el registro de auditoría y la prueba de reproducción como CSV; solicite el registro de la última limpieza por plazo de conservación. Cada prueba requiere unos minutos y le dice a un comité más que cualquier lista de funciones.

10 Acerca de taleor

Con taleor, usted gestiona un espacio de experiencias de forma segura y agéntica: su contenido, sus aplicaciones interactivas, sus pantallas y su hardware, desde una sola consola, en la nube, en un servidor local o totalmente aislado de la red. Está dirigido a museos, centros de ciencia, centros de experiencia de marca, sitios patrimoniales y atracciones, y a las personas que los gestionan y se encargan de sus compras.

taleor se lanza en noviembre de 2026. Escriba a hello@taleor.net para organizar un proyecto piloto o solicitar la ficha técnica para licitaciones en cualquiera de nuestros siete idiomas: inglés, alemán, neerlandés, polaco, francés, español o italiano.

Fuentes y verificación

Cada afirmación técnica de este documento se basa en una fuente identificada en el código, los documentos de diseño o la revisión de seguridad de taleor, recogida en un registro de afirmaciones que enumera cada afirmación, la sección en la que aparece y el archivo del que procede. Escriba a hello@taleor.net para solicitar el registro.

Referencias públicas utilizadas en la sección 2, ninguna con cifras: la botnet Mirai de 2016 (ampliamente documentada, entre otros por la Cybersecurity and Infrastructure Security Agency de EE. UU.); BSI IT-Grundschutz (Alemania); la Baseline Informatiebeveiliging Overheid (Países Bajos); la Directiva (UE) 2022/2555, conocida como NIS2; y los requisitos básicos (Baseline Requirements) del CA/Browser Forum para la vigencia de 398 días de los certificados.

