



Condiciones de alta, acceso y uso del Espacio de Datos ED-AECPD

1. Objeto y alcance

Este documento recoge, de forma práctica, las condiciones para darse de alta, acceder y usar el portal del Espacio de Datos ED-AECPD (en adelante, el “Espacio”). Aplica a todas las organizaciones y usuarios autorizados. La adhesión y las operaciones relevantes (publicación y obtención/descarga) requieren una aceptación expresa de estas condiciones en el propio portal.

El Espacio está orientado a ofrecer servicios de valor (benchmarking, informes ejecutivos, alertas y descargas) a partir de datos económicos y operativos agregados por sector y periodo. El objetivo es que el intercambio sea sencillo de usar, pero gobernado: reglas claras, control de acceso y evidencias de lo que ocurre (quién publica, quién obtiene, cuándo y bajo qué condiciones).

2. Roles y conceptos básicos

En el Espacio existen cuatro roles operativos. Un mismo participante puede tener más de un rol si el Operador lo autoriza: Participante (organización adherida), Productor (publica datos), Consumidor (obtiene productos/servicios) y Operador/Autoridad de Gobierno (AECPD, que gobierna y opera el Espacio).

A efectos de trazabilidad, el sistema genera “evidencias” (normalmente en formato JSON) para operaciones como la publicación y la descarga. Estas evidencias incluyen una marca temporal y una huella criptográfica (SHA-256) del fichero para poder verificar su integridad.

3. Operativa del Espacio AECPD

El ciclo de vida del ED-AECPD es: la organización solicita adhesión y acepta condiciones; se le asigna un rol (Productor y/o Consumidor) y se activa el acceso; el Productor envía un fichero mensual que queda en revisión; una vez publicado, el Consumidor selecciona un servicio del catálogo, elige intervalo y formato y obtiene el entregable; y el sistema conserva evidencias de publicación y de obtención y descarga para auditoría y resolución de incidencias.

4. Adhesión y activación de acceso

La adhesión se realiza desde el portal mediante un formulario de alta. El Participante debe identificarse como organización, indicar un contacto y seleccionar el rol solicitado. La solicitud queda registrada y puede requerir revisión por el Operador antes de activarse.

La activación implica asignar roles y permisos mínimos. Para perfiles privilegiados (operación, administración o auditoría) el Operador puede exigir medidas adicionales como MFA y restricciones de sesión.

Las condiciones económicas aplicables se recogen en el documento “**Condiciones económicas y comerciales**”, que el participante acepta expresamente durante el proceso de adhesión. Para casos especiales (p. ej., cambios de rol, alta/baja parcial, volúmenes no estándar o servicios a medida), las condiciones deberán consultarse y validarse previamente con el Operador, quedando constancia de la aceptación correspondiente.

5. Publicación por parte del Productor (solo CSV mensual)

El Productor publica un único tipo de aportación: un fichero CSV mensual con datos agregados, siguiendo el esquema del Espacio. No se admiten otros formatos ni anexos documentales (por ejemplo, PDFs, hojas de cálculo adicionales o informes).

El CSV incluye campos contables y operativos agregados (por ejemplo, ingresos, costes, márgenes, estructura de gastos), métricas agregadas de RRHH (por ejemplo, empleados, altas/bajas, rotación, absentismo) y, cuando aplique, extensiones específicas por sector. El Productor es responsable de que el fichero sea coherente, consistente con el diccionario del Espacio y que no incorpore datos personales como contenido del producto.

La publicación se tramita como “envío a revisión”. El sistema registra el envío, calcula la huella SHA-256 del fichero y genera una evidencia de publicación. El Operador puede rechazar o devolver a corrección si faltan campos, si hay incoherencias o si el nivel de agregación genera riesgo de inferencia.

6. Obtención por parte del Consumidor (catálogo y transacción)

El Consumidor accede al catálogo autenticado, selecciona un servicio (p. ej., benchmarking, alertas, informes o descargas), define el intervalo temporal y el formato de salida (CSV/JSON o visualización). Antes de obtener el producto, debe aceptar las condiciones de uso aplicables; esa aceptación queda registrada.

La descarga o entrega genera una evidencia de transacción. Si el acceso no cumple las condiciones (rol insuficiente, producto no habilitado, o incumplimiento de reglas), el sistema deniega la operación y registra la denegación.

7. Reglas de uso (condiciones esenciales)

El uso de los productos del Espacio es interno y para la finalidad declarada. No se permite la redistribución a terceros ni la reventa. También se prohíben expresamente los intentos de inferencia o reidentificación (por ejemplo, cruzar el dataset con otras fuentes para identificar a una organización o deducir información sensible).

Los participantes deben mantener confidencialidad, proteger el acceso de sus usuarios y notificar incidentes o accesos no autorizados cuando los detecten. El Operador puede suspender accesos si existe riesgo, incumplimiento o necesidad de contención.

8. Privacidad, minimización y control de inferencia

Como regla general, los productos del catálogo se diseñan para no incluir datos personales en su contenido: son datos agregados por organización/sector/periodo y con controles frente a riesgo de inferencia. Aun así, el Espacio necesita registrar ciertos datos operativos para funcionar (por ejemplo, usuario/rol, marcas temporales y metadatos técnicos de la transacción) con fines de autenticación, control de acceso e auditoría.

Para reducir el riesgo de inferencia, el Operador aplica una regla mínima: no se publicarán entregas que contengan grupos con tamaño inferior a un umbral operativo (k). Por defecto, el umbral es $k=5$; si un conjunto no lo cumple, se agregará a un nivel superior o se suprimirá la salida afectada. Este criterio puede ajustarse por sector si el Comité Técnico-Seguridad lo aprueba.

9. Trazabilidad, evidencias e integridad

El Espacio genera evidencias en formato estructurado (JSON) para operaciones clave: adhesión, publicación, revisión/aprobación, obtención/descarga y denegaciones. Cada evidencia incluye, como mínimo, el tipo de evento, la fecha/hora y la referencia al recurso entregado, y cuando aplica la huella SHA-256 del fichero. Estas evidencias permiten reconstruir qué ocurrió y verificar integridad (el fichero descargado coincide con el publicado). El Operador procura que las evidencias no incluyan contenido sensible; los campos técnicos (como IP o user-agent) se tratan como metadatos operativos y se gestionan con minimización y retención.

10. Retención, borrado y copias de seguridad

El Espacio aplica retención limitada y borrado conforme a finalidad. Con carácter orientativo: evidencias de publicación y descarga y registros de auditoría se conservan 24 meses; logs técnicos de seguridad se conservan 12 meses; y las copias de seguridad se conservan 30 días, salvo necesidad de restauración. Estos plazos pueden ajustarse por obligación legal o por requerimientos de auditoría, y cualquier cambio relevante se documentará.

Los participantes se comprometen a respetar la retención definida para cada producto. Cuando expire el plazo, deberán borrar o anonimizar internamente cualquier copia bajo su control, salvo obligación legal que justifique conservación superior.

11. Incidencias, incumplimientos y medidas

Las incidencias se gestionan con un procedimiento simple: registro, análisis, propuesta de resolución y comunicación a las partes. Si hay riesgo para la seguridad o incumplimiento de condiciones, el Operador puede aplicar medidas provisionales (por ejemplo, suspensión temporal de acceso) hasta su cierre.

Los incumplimientos graves (redistribución, intentos de inferencia/reidentificación, manipulación de evidencias o accesos no autorizados) pueden implicar suspensión, revocación de acceso y, en su caso, la expulsión del Espacio conforme al rulebook.

12. Baja (offboarding) y salida ordenada

Un participante puede solicitar baja. La salida ordenada incluye: revocación de accesos, cierre de cuentas de usuario, y retirada de permisos futuros. Los productos ya obtenidos deberán borrarse conforme a los plazos de retención y a las obligaciones asumidas.

El Operador puede conservar, durante los plazos de retención definidos, las evidencias y registros necesarios para demostrar operaciones realizadas y para atender auditorías o incidencias abiertas. Si el participante era Productor, sus publicaciones históricas podrán mantenerse en el catálogo durante el periodo acordado, o retirarse si así lo determinan las reglas del Espacio y el impacto sobre consumidores autorizados.

AECPD puede actualizar este documento para mejorar seguridad, gobernanza o claridad operativa. Los cambios se comunicarán a los participantes y, cuando sean sustanciales, requerirán nueva aceptación en el portal antes de continuar operando.