

PROTOCOLO USO DE LAS SALAS SEGURAS DEL ICPM

PRIMERO.- OBJETIVO Y ALCANCE

El objetivo del documento es establecer los criterios a seguir para la aplicación preferente de los medios telemáticos que rijan las actuaciones procesales no presenciales. Se trata de establecer un conjunto homogéneo de requisitos mínimos a cumplir, así como recomendaciones técnicas de las aplicaciones, tanto en las relaciones internas de los órganos de la Administración de Justicia, como fuera de ella, sin que en ningún caso se limiten, obstaculicen o impidan las garantías del proceso.

1.1.- Actuaciones procesales no presenciales.

Las actuaciones procesales no presenciales se refieren a las vistas de juicios, las comparencias, audiencias y otras actuaciones que tienen lugar total o parcialmente sin la presencia de alguna de las personas o profesionales que intervienen en ella, bien mediante sistemas de videoconferencia o a través de una sala virtual creada al efecto.

Tradicionalmente, las vistas y el resto de las actuaciones procesales se han celebrado de forma presencial. La reforma del artículo 229 de la Ley Orgánica del Poder Judicial, abre la posibilidad de realizar vistas mixtas. En este tipo de vistas, algunas de las actuaciones se celebran telemáticamente, como, por ejemplo: las declaraciones, interrogatorios, testimonios, careos, exploraciones, informes, ratificación de las pruebas periciales, bien mediante sistemas de videoconferencia, siendo el resto practicadas presencialmente.

Por extensión se han comenzado a realizar otras actuaciones procesales, como comparencias o audiencias, donde alguno de los participantes no está presente físicamente en las dependencias del órgano judicial y se conecta con el mismo por sistemas telemáticos. De este modo, las actuaciones procesales mixtas se incorporan a la realidad de la práctica de la Administración de Justicia.

Posteriormente el Real Decreto Ley 16/2020, de 28 de abril, contempló la forma telemática como el modo preferente de celebración de las actuaciones judiciales, aunque limitado en el tiempo. Fuera del periodo previsto en el Real Decreto, el juez o magistrado por razones organizativas, de flexibilidad, accesibilidad o como opción preferente frente a un aplazamiento o suspensión, podrá acordar la celebración de la actuación procesal, mediante videoconferencia sin la presencia física de ninguno de los intervinientes en la sede o dependencia del juzgado o tribunal.

Las vistas y actuaciones no presenciales que se celebran por vía telemática en su totalidad deben respetar en todo caso los principios de publicidad, intermediación, oralidad y el resto de las garantías del proceso.

La Ley Orgánica del Poder Judicial posibilita las actuaciones por videoconferencia u otro sistema similar, siempre que permita la comunicación bidireccional y simultánea de la imagen y el sonido y la interacción visual, auditiva y verbal entre dos personas o grupos de personas geográficamente distantes, asegurando en todo caso la posibilidad de contradicción de las partes y la salvaguarda del derecho de defensa, cuando así lo acuerde el juez o tribunal.

SEGUNDO.- PUNTOS DE ACCESO SEGUROS

En el artículo 62 del Real Decreto-ley 6/2023 se definen los puntos de acceso seguros como aquellos dispositivos y sistemas de información, que cumplan con los requisitos que se recogen en esta norma, y que en todo caso reunirán, al menos, los siguientes:

- a) Permitir la transmisión segura de las comunicaciones y la protección de la información.
- b) Permitir y garantizar la identificación de los intervinientes.
- c) Cumplir los requisitos de integridad, interoperabilidad, confidencialidad y disponibilidad de lo actuado.

Estos requisitos mínimos, deben adoptar mayor concreción dado su carácter genérico, y adecuarse a los niveles de seguridad, en las diferentes dimensiones de seguridad, exigibles a los sistemas de información a través de los que se materializan, de forma telemática, las actuaciones procesales, y la atención y servicios no presenciales al público y a los profesionales, en función de la criticidad de la información, incluidos los datos personales, y del servicio que se presta.

Con este propósito se establecen los siguientes requisitos de seguridad, sin perjuicio de la aplicación del resto de los controles o medidas técnicas y organizativas aplicables del Anexo II del Esquema Nacional de Seguridad (ENS).

2.1.- Requisitos mínimos de seguridad.

En cuanto a las instalaciones, dónde se encuentran los dispositivos y equipos utilizados para la conexión a los sistemas de videoconferencia o similares provistos por las administraciones prestacionales, deben cumplir los siguientes requisitos mínimos:

- a) Los dispositivos y los equipos utilizados para las conexiones, así como los equipos necesarios para las comunicaciones, deben ubicarse en áreas de acceso restringido, protegidas mediante controles de entrada, adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.
- b) Los despachos deberán estar cerrados bajo llave, custodiada únicamente por la persona a la que pertenece dicho despacho y por el personal de seguridad y deberán permanecer cerrados con llave cuando las personas se ausenten de los mismos.
- c) La información confidencial u objeto de intercambio, o los soportes de información extraíbles, se almacenará en armarios y archivadores que cuenten con cerradura y deberán permanecer cerrados tras finalizar la jornada laboral y, siempre que no se esté haciendo uso de los mismos.
- d) Las visitas, previamente identificadas por medio de DNI o documento equivalente, deberán estar en todo momento acompañadas por personal interno, y la información confidencial no estará visible ni accesible para los visitantes no autorizados.
- e) Se deben considerar sistemas de detección de intrusos a las instalaciones.

La implantación y cumplimiento de estos requisitos mínimos se realizará de acuerdo con el Esquema Nacional de Seguridad, siguiendo las guías, recomendaciones y buenas prácticas del Centro Criptológico Nacional (CCN).

2.2.- Características técnicas y requisitos de uso.

Este proyecto se lleva a cabo respetando los requisitos mínimos establecidos en el Real Decreto-ley 6/2023, de 19 de diciembre.

2.2.1.- Se lleva a cabo la adquisición de medios audiovisuales para cumplir los requisitos mínimos técnicos:

- a) La calidad de la imagen de la persona que va a realizar el acto con la suficiente nitidez para su identificación física y expresión facial por todos los participantes de la videoconferencia. Para ello, la cámara deberá permitir la reproducción como mínimo de vídeo Full HD 1080p. Además, asegurará la posibilidad de, cuando así sea requerido, tener una imagen más amplia del participante en la actuación procesal (incluyendo brazos e incluso cuerpo).
- b) La calidad del sonido para evitar distorsiones y acoples de sonido. Para ello, se recomienda el uso de auriculares con micrófono. Si no es posible, se dispondrá de un micrófono externo. Para evitar el ruido de fondo, se recomienda el uso de auriculares con cancelación de ruido. La señal de audio digital de al menos 24 bits.

2.2.2.- Se configuran los dispositivos de comunicaciones de acuerdo a:

- a) Conexión a internet con el suficiente ancho de banda para garantizar los anteriores requisitos de calidad de imagen y sonido. El ancho de banda mínimo requerido será de 100 Mbps. Cuando sea posible, se recomienda conectar el dispositivo con cable en lugar del uso de WIFI.

2.2.3.- Se configuran equipos para cumplir:

Los dispositivos y equipos utilizados para la conexión a los sistemas de videoconferencia o similares provistos por las administraciones prestacionales, deben cumplir los siguientes requisitos mínimos:

- a) El sistema operativo tiene, al menos, instalada la última versión validada para su uso.
- b) El sistema operativo tiene instaladas las actualizaciones de seguridad.
- c) El equipo tiene instalado y activado un sistema antimalware, que escanea tanto el propio equipo, como cualquier unidad externa que se le conecte.
- d) El equipo tiene instalado y activado un sistema cortafuegos para bloquear tráfico no autorizado.
- e) La red a la que se conecta el equipo tiene instalado y activado un sistema de detección de intrusiones para detectar tráfico no autorizado.
- f) El equipo no tiene instaladas aplicaciones de origen desconocido o no confiable.
- g) Todo equipo cuenta, como mínimo, con un mecanismo de autenticación de, al menos, un factor (por ejemplo, contraseña).
- h) Los usuarios que acceden al equipo quedan identificados singularmente, de tal forma que se puede saber quién es y qué derechos de acceso tiene.
- i) Los usuarios que acceden al equipo tienen asignadas credenciales de acceso únicas.
- j) A las contraseñas se les aplican normas de complejidad mínima y robustez frente a ataques de adivinación.
- k) El número de intentos permitidos es limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta.
- l) Se registra la actividad de los usuarios dentro del equipo, de manera que se refleja la actividad que éstos realizan, el momento y la información sobre la que se haga.
- m) Sólo el personal autorizado tiene derechos de acceso a dichos registros.

- n) Se bloquea el equipo o dispositivo tras un periodo de inactividad; del mismo modo, toda sesión activa, se cancela tras un periodo de inactividad.
- o) Para acceder a un equipo o dispositivo que ha sido bloqueado por inactividad se requerirá la autenticación de usuario.

2.2.4.- Se firma el documento de Declaración Responsable para la homologación.

2.2.5.- De acuerdo con el procedimiento de declaración responsable, se realizan las pruebas de conexión mediante videoconferencia con el listado que nos proporcionan desde el CTEAJE, un total de 13 Administraciones.

2.2.6.- Finalmente, habiendo resultado satisfactorio el cumplimiento de todos los requisitos, se nos incluye en el listado de entidades que han declarado su conformidad con la GIS de Requisitos de puntos de acceso seguro y lugares seguros.

2.3.- Hoja de Registro de utilización de las Salas.

Juzgado	Autos	Territorio



DNI	Apellidos y Nombre	Como	Firma	Hora Entrada	Hora Salida

DNI	Apellidos y Nombre	Como	Firma	Hora Entrada	Hora Salida

DNI	Apellidos y Nombre	Como	Firma	Hora Entrada	Hora Salida

DNI	Apellidos y Nombre	Como	Firma	Hora Entrada	Hora Salida

PROTECCIÓN DE DATOS: En virtud de la normativa vigente de protección de datos de carácter personal compuesta por el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (RGPD) y la Ley 3/2018 de 5 de diciembre sobre protección de datos y garantía de derechos digitales (LOPDGDD) le informamos que el responsable del tratamiento es el Ilustre Colegio de Procuradores de Madrid (ICPM) para la finalidad de utilización y uso por el solicitante de la sala segura para la realización de vistas y señalamientos en virtud del artículo 62 de del R.D 6/2023 de 19 de diciembre por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. Asimismo, le informamos que puede ejercitar sus derechos reconocidos en la normativa de protección de datos mencionado dirigiéndose a nosotros en el email: dpo@icpm.es, asimismo, pueden obtener mayor información sobre la política de privacidad del ICPM en www.icpm.es

2.4.- Tarifas por utilización espacios Salas Seguras.

Las tarifas por el uso de la Sala Segura serán las siguientes:

20€/hora + IVA → usuario: Procuradores adscritos ICPM (Por cada 30 minutos o fracción adicional se cobrará un 25% más)

50€/hora + IVA → usuario: Procuradores adscritos ICPM acompañado Abogados / Otros (Por cada 30 minutos o fracción adicional se cobrará un 50% más)

50€/hora + IVA → usuario: Procuradores de otros colegios / Abogados / Otros (Por cada 30 minutos o fracción adicional se cobrará un 50% más)

El abono por la reserva de sala se realizará previa solicitud, y se aportará el justificante de transferencia con la misma. Puede realizar el pago a través de transferencia bancaria, BANCO SANTANDER - número de cuenta ES72 0075 0322 8206 0039 8913 del ICPM, USO SALA SEGURA “NOMBRE”

- * El pago será por parte del usuario de la sala no por el solicitante.
- * Facturación mínima de 1 hora, el abono por uso adicional se realizará terminado el uso de la sala.
- * Únicamente se devolverá la reserva por resolución judicial de suspensión o no autorización de la celebración del acto a través de este medio.
- * Se abonará por el profesional interviniente salvo indicación de facturar a nombre de un tercero.

Madrid, 24 de junio de 2025