CTEAJE

Comité Técnico Estatal de la Administración Judicial Electrónica

GUÍA TÉCNICA DE INTEROPERABILIDAD Y SEGURIDAD DE REQUISITOS DE PUNTOS DE ACCESO SEGURO Y LUGARES SEGUROS

CTEAJE
Comité Técnico Estatal de la Administración Judicial Electrónica

Ficha del Documento

GRUPO DE TRABAJO	Haga clic para escribir texto
NOMBRE DEL DOCUMENTO	GUÍA TÉCNICA DE INTEROPERABILIDAD Y SEGURIDAD DE REQUISITOS DE PUNTOS DE ACCESO SEGURO Y LUGARES SEGUROS
CÓDIGO DEL DOCUMENTO	Haga clic para escribir texto
VERSIÓN	1.3

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	Oficina de Seguridad CTEAJE	23/03/2023	Versión inicial. Se aprueba en el Subcomité de Seguridad de 23/03/2023 (LED pendiente de aprobación).
1.1	Oficina de Seguridad CTEAJE	21/12/2023	Adecuación al Real Decreto-ley 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.
1.2	Oficina de Seguridad CTEAJE	26/02/2024	Se identifican los requisitos mínimos funcionales, técnicos y de seguridad que deben cumplir los puntos de acceso y lugares seguros. Versión presentada en la Comisión Permanente del 7 de marzo de 2024 y posteriormente aprobada.
1.3	Oficina de Seguridad CTEAJE	09/04/2024	Se realizan correcciones gramaticales. Se modifica la redacción del contenido de los puntos 5.1 (identificación) y 5.2 (cumplimiento de requisitos mínimos).

Índice

1. INTRODUCCIÓN

Con la entrada en vigor del Real Decreto-ley 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, la consolidación de la vía telemática para la generalidad de las actuaciones procesales en los órganos jurisdiccionales, con la excepciones recogidas, requiere la regulación y definición, mediante requisitos técnicos y de garantía, de los llamados «puntos de acceso seguros» y los «lugares seguros» desde los que se podrán efectuar con plenos efectos procesales las intervenciones telemáticas, en los términos que disponen las modificaciones de las leyes procesales, con objeto de preservar la inmediación digital en todas las actuaciones mediante videoconferencia.

Asimismo, se establece que la atención y servicios no presenciales al público y a los profesionales se realizará desde un punto de acceso seguro.

De acuerdo con lo anterior, se modifican las normas procesales, estableciéndose que la intervención, ante el juez o Tribunal, ante los letrados de la Administración de Justicia o ante el Ministerio Fiscal, mediante presencia telemática se practicará siempre a través de punto de acceso seguro, de conformidad con la normativa que regule el uso de la tecnología en la Administración de Justicia. Ambas normas coinciden establecer para los intervinientes en su condición de autoridad o funcionario público, su intervención desde un punto de acceso seguro.

La Ley de Enjuiciamiento Civil prevé, de acuerdo con los requisitos previstos, la intervención mediante presencia telemática en un lugar seguro dentro del municipio de residencia que fuera distinto del lugar de la sede del tribunal, de conformidad con la normativa que regule el uso de la tecnología en la Administración de Justicia.

En el ámbito penal, las víctimas de violencia de género, de violencia sexual, de trata de seres humanos, víctimas menores de edad o con discapacidad, podrán intervenir desde los lugares donde se encuentren recibiendo oficialmente asistencia, atención, asesoramiento o protección, o desde cualquier otro lugar, siempre que dispongan de medios suficientes para asegurar su identidad y las adecuadas condiciones de la intervención.

El Real Decreto-ley 6/2023, de 19 de diciembre, encomienda y faculta al Comité técnico estatal de la Administración judicial electrónica (CTEAJE) a determinar los requisitos técnicos y de garantía de los «puntos de acceso seguros» y los «lugares seguros» a través de su normativa, respetando aquellos mínimos establecidos en la citada ley.

Además de los requisitos, dicho real decreto-ley establece en todo caso una relación de lugares seguros, que podrá ser ampliada por medio de su desarrollo reglamentario para todo el Estado, previo informe favorable del CTEAJE.

2. OBJETIVO

La Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros tiene por objeto determinar los requisitos técnicos y de garantía que deben tener los puntos de acceso seguros y lugares seguros, respetando los requisitos mínimos establecidos en el Real Decreto-ley 6/2023, de 19 de diciembre, de acuerdo con el mandato al CTEAJE previsto en la misma.

3. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la presente guía técnica es todo el territorio del Estado.

4. 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).

4.1 Usuarios internos y externos

El ENS diferencia los mecanismos de autenticación para los usuarios internos, o de la organización, y para los usuarios externos, y en función del nivel de seguridad de las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad.

A efectos de esta Guía Técnica, se entenderá por usuarios internos aquellos colectivos a los que las Administraciones con competencia en materia de provisión de medios personales y materiales de la Administración de Justicia, tienen la obligación legal de suministrar todos los

medios técnicos necesarios para que puedan desempeñar sus funciones, y por tanto tienen un control sobre los mismos.

En este sentido, tendrán la **condición de usuarios internos**, los siguientes colectivos, o el personal que presta servicios en los siguientes órganos:

- Órganos judiciales y fiscales
- Oficinas judiciales y fiscales
- Oficinas de Justicia en el Municipio
- Oficinas de Registro Civil
- Instituto Nacional de Toxicología y Ciencias Forenses
- Institutos de Medicina Legal

Con los mismos efectos anteriores, tendrán la **condición de usuarios externos** los siguientes:

- Ciudadanos
- Profesionales
- Fuerzas y Cuerpos de Seguridad del Estado
- Centros penitenciarios y órganos dependientes de Instituciones Penitenciarias
- Centros de internamiento de extranjeros
- Centros de internamiento de menores
- Otros no considerados internos

4.2 Zona controlada y no controlada

Por otro lado, se requerirán diferentes mecanismos de autenticación en función del acceso al sistema, por parte de los usuarios internos, desde una zona controlada o no controlada.

De acuerdo con el ENS, se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso puntual al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

A efectos de esta Guía Técnica, tendrá la **condición de zona controlada**, las sedes físicas donde realizan sus funciones los colectivos considerados usuarios internos (de forma presencial, sin considerar el teletrabajo). Desde estas sedes o zonas controladas, el tráfico entre el cliente y el servidor se realiza solo a través de las redes internas provistas por las Administraciones prestacionales.

4.3 Mecanismos de autenticación

Usuarios internos

- **Acceso desde zonas controladas:** Cualquiera de los previstos en el Anexo II del ENS [op.acc.6]:

  - Contraseñas

  - Contraseña + otro factor de autenticación (“algo que se tiene” o “algo que se es")

  - Certificados (cualificados, protegidos por segundo factor)

  - Certificados en dispositivo físico (cualificados, protegidos por segundo factor)

- **Acceso desde zonas no controladas:** se establece el **doble factor de autenticación** para los usuarios internos que accedan desde o a través de zonas no controladas, de acuerdo con las opciones de doble factor previstas en la medida [op.acc.6] del Anexo II del ENS.

Usuarios externos

- **Acceso desde zonas controladas:** aunque el ENS no distingue zona controlada en el caso de usuarios externos, en esta Guía debemos diferenciar las actuaciones procesales telemáticas donde el usuario externo se presenta en alguna sede física donde realizan sus funciones los usuarios internos (al servicio de la Administración de Justicia), y que, por tanto, es una zona controlada. La identificación se realiza de manera física a través del documento identificativo.

- **Acceso desde zonas no controladas:** se establece el **doble factor de autenticación** para los usuarios a través de los mecanismos de autenticación previstos en el Anexo II del ENS [op.acc.5] de nivel medio o alto:

  - Contraseña + otro factor de autenticación (“algo que se tiene” o “algo que se es")

  - Certificados (cualificados, protegidos por segundo factor)

  - Certificados en dispositivo físico (cualificados, protegidos por segundo factor)

4.4 Requisitos mínimos técnicos

A efectos de esta Guía Técnica, tendrá **la condición de puntos de acceso seguros los que acrediten el cumplimiento de los siguientes requisitos**:

- el encriptado punto a punto de las comunicaciones.

- 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).

- 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.

- 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.

4.5 Requisitos mínimos de seguridad

Se definen los siguientes requisitos mínimos para la consideración de puntos de acceso seguro de acuerdo con el artículo 62.2. La verificación de estos requisitos podrá ser objeto de auditoría por parte del Subcomité de Seguridad del CTEAJE.

1 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.
    i. Sólo el personal autorizado tiene derechos de acceso a dichos registros.
m. Se bloquea el equipo o dispositivo tras un periodo de inactividad; del mismo modo, toda sesión activa, se cancela tras un periodo de inactividad.
    i. Para acceder a un equipo o dispositivo que ha sido bloqueado por inactividad se requerirá la autenticación de usuario.

2 Se debe disponer de un procedimiento de gestión de incidentes de seguridad de la información y protección de datos personales, que incluya la obligación de notificar lo antes posible una brecha de seguridad que pueda haber afectado a la confidencialidad de las actuaciones telemáticas mantenidas con la Administración de Justicia, incluida la información que pueda haber sido intercambiada con la misma, al Servicio de Gestión de Incidentes de CTEAJE (incidentes.cteaje@mju.es).

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).

Los requisitos anteriores podrán considerarse cumplidos con la presentación de certificación de conformidad con el Esquema Nacional de Seguridad, o de otras certificaciones equivalentes en materia de seguridad de la información (p.ej. ISO27001), sin necesidad, en ese caso, de presentar declaración responsable de cumplimiento. El alcance de tales certificaciones debe incluir los dispositivos y equipos a los que aplican estos requisitos mínimos de seguridad.

5. LUGARES SEGUROS

El artículo 62 del Real Decreto-ley 6/2023, de 19 de diciembre, define los lugares seguros como aquellos que cumplan con los requisitos que se recogen en esta norma, y que en todo caso reunirán, al menos, los siguientes:

a) Disponer de dispositivos y sistemas que tengan la condición de punto de acceso seguro, conforme al apartado anterior.

b) Garantizar la comprobación de la identidad de los intervinientes y la autonomía de su intervención.

c) Asegurar todas las garantías del derecho de defensa, inclusive la facultad de entrevistarse reservadamente con el Abogado o Abogada.

d) Disponer de medios que permitan la digitalización de documentos para su visualización por videoconferencia.

Además, el citado real decreto-ley establece una **relación de lugares seguros** en todo caso:

a) La oficina judicial correspondiente al tribunal competente, o cualquier otra oficina judicial o fiscal, y las oficinas de justicia en el municipio.

b) Los Registros Civiles, para actuaciones relacionadas con su ámbito.

c) El Instituto Nacional de Toxicología y Ciencias Forenses y los Institutos de Medicina Legal, para la intervención de los Médicos Forenses, Facultativos, Técnicos y Ayudantes de Laboratorio.

d) Las sedes de las Fuerzas y Cuerpos de Seguridad del Estado, para la intervención de sus miembros.

e) Las sedes oficiales de la Abogacía del Estado, del Servicio Jurídico de la Administración de la Seguridad Social y de los Servicios Jurídicos de las Comunidades Autónomas, para la intervención de los miembros de tales servicios.

f) Los Centros penitenciarios, órganos dependientes de Instituciones Penitenciarias, centros de internamiento de extranjeros y centros de internamiento de menores, para las personas internas y funcionarios públicos.

g) Cualesquiera otros lugares que se establezcan por Reglamento de aplicación en todo el territorio del Estado, previo informe favorable del Comité técnico estatal de la Administración judicial electrónica.

5.1 Requisitos mínimos funcionales y técnicos

A efectos de esta Guía Técnica, tendrá **la condición de lugares seguros** las zonas controladas identificadas en el apartado anterior, las zonas no controladas ya incluidas en la relación de lugares seguros por el citado Real Decreto-ley, aquellos que reglamentariamente se establezcan, previo informe favorable del CTEAJE, y **aquellos otros lugares que acrediten el cumplimiento de los siguientes requisitos mediante declaración responsable**:

- el cumplimiento del resto de requisitos mínimos.
- el cumplimiento de la prohibición de grabar, tomar imágenes o registrar sonido de tales actuaciones, advirtiendo que en caso de incumplimiento podrá incurrirse en la responsabilidad que legalmente se determine.
- el cumplimiento de las condiciones de privacidad, garantía de ausencia de terceras personas e inexistencia de influencia externa alguna durante la práctica de la prueba, conforme establece la legislación procesal.
- la no aplicación de sistemas o aplicaciones que alteren o distorsionen la imagen y el sonido transmitido, salvo en los casos previstos legalmente.

- el cumplimiento de la integridad y autonomía de la declaración del interviniente, mediante la visualización de la estancia completa en la que se realice, así como las condiciones ambientales de la misma, en el caso que sea requerido.

- la identificación de los intervinientes se realizará mediante los sistemas de identificación admitidos por la Administración de Justicia de conformidad con el Real Decreto-ley 6/2023, de 19 de diciembre.

En los supuestos en los que el interviniente carezca de los anteriores sistemas de identificación, ésta podrá ser efectuada siempre que sea posible desde un punto de vista procesal[1], por personal integrante del lugar seguro.

- el contacto con las personas que se van a conectar desde el lugar seguro mediante teléfono y correo electrónico que deberá haber sido proporcionado con anterioridad al órgano judicial o fiscalía.

5.2 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.
    i. 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.
    i. 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).

[1] Se hace referencia a labores asistenciales de la identificación, y en su caso la comprobación de la identidad en supuestos procesales en los que sea autorizado por el Juez o Magistrado.

Los requisitos anteriores podrán considerarse cumplidos con la presentación de certificación de conformidad con el Esquema Nacional de Seguridad, o de otras certificaciones equivalentes en materia de seguridad de la información (p.ej. ISO27001), sin necesidad, en ese caso, de presentar declaración responsable de cumplimiento. El alcance de tales certificaciones debe incluir las instalaciones a las que aplican estos requisitos mínimos de seguridad.