CTEAJE

Comité Técnico Estatal de la Administración Judicial Electrónica

GUÍA DE CRITERIOS DE VALORACIÓN DE REFERENCIA DE DIMENSIONES DE SEGURIDAD

CTEAJE

Ficha del Documento

NOMBRE DEL DOCUMENTO	GUÍA DE CRITERIOS DE VALORACIÓN DE REFERENCIA DE DIMENSIONES DE SEGURIDAD
VERSIÓN	1.0

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	Oficina de Seguridad CTEAJE	Aprobada en Subcomité de Seguridad 27/06/2024 Aprobada en Pleno 21/11/2024	Versión inicial del documento. Se presenta en Subcomité de Seguridad de 10/05/2024. Aprobada en Pleno 21/11/2024

Índice

1. INTRODUCCIÓN

De acuerdo con la metodología del Esquema Nacional de Seguridad (ENS) y del Esquema judicial de interoperabilidad y seguridad (EJIS), la aplicabilidad de las medidas de seguridad en un sistema de información depende de dos factores: la valoración de las dimensiones de seguridad[1] (niveles BAJO, MEDIO, ALTO) y la categoría de seguridad del sistema (BÁSICA, MEDIA, ALTA), que vendrá determinada por el nivel más alto de las dimensiones valoradas[2]. Existen medidas que son aplicables en función del nivel de seguridad de sus dimensiones o en función de la categoría del sistema.

Para efectuar las valoraciones de las dimensiones de seguridad, el Anexo I del ENS requiere que se lleve a cabo la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Garantizar la conformidad con el ordenamiento jurídico.

Estos tres elementos constituyen criterios de valoración del impacto de un incidente de seguridad.

Asimismo, el ENS establece la posibilidad de aplicar otros criterios análogos, incluido el perjuicio a los individuos.

La Guía CCN-STIC-803 *Valoración de Sistemas*[3] en el ENS recoge un conjunto de criterios, comunes a todas las dimensiones y otros específicos, por afectar a alguna dimensión, por estar afectados por regulaciones especiales, o bien son criterios adaptados a un ámbito concreto.

Tipología	Criterios
Generales o comunes a todas las dimensiones de seguridad	a) Alcanzar sus objetivos. b) Proteger los activos a su cargo. c) Garantizar la conformidad con el ordenamiento jurídico. Análogos: ▪ Perjuicio Directo al ciudadano ▪ Pérdidas económicas ▪ Reputación ▪ Protestas ▪ Delitos
Para tipos de información con datos personales	Protección de los derechos fundamentales de los titulares de los datos personales

[1] Confidencialidad, Integridad, Autenticidad, Trazabilidad y Disponibilidad.
[2] Si el nivel mayor de alguna dimensión es ALTO, la categoría del sistema será ALTA; en caso de ser MEDIO, la categoría será MEDIA; y en caso de ser BAJO, la categoría será BÁSICA.
[3] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html

Tipología	Criterios
Para la disponibilidad de los servicios	Periodos críticos RTO (Tiempo de recuperación objetivo)
Criterios específicos (Universidades)	Guía de Seguridad de las TIC CCN-STIC 803 Anexo I – Valoración de los sistemas en Universidades[4].
Criterios específicos para operadores críticos del sector público	Será la Secretaría de Estado de Seguridad a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) la que establezca reglamentariamente los criterios a emplear para la protección de los servicios esenciales de las infraestructuras designadas como críticas en los correspondientes planes estratégicos sectoriales

2. OBJETO

El 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 -art.85.2 e)-, y la Política de Seguridad de la Información de la Administración Judicial Electrónica (PSIAJE) -art. 8.2b-, encomiendan al Comité técnico estatal de la Administración judicial electrónica (CTEAJE), a través del Subcomité de Seguridad, la definición y el establecimiento de criterios de valoración de referencia que determinen el nivel de seguridad de cada dimensión de seguridad.

Por tanto, el presente documento tiene por objeto dar cumplimiento a dicho mandato, estableciendo los criterios de valoración específicos en el ámbito de los sistemas de información de la Administración de Justicia.

3. SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN DE JUSTICIA

De acuerdo con la PSIAJE, se establece la siguiente diferenciación o clasificación de sistemas de información en el ámbito de la Administración de Justicia:

- Sistemas de información de Juzgados y Tribunales
- Sistemas de información de Fiscalías
- Sistemas auxiliares:
  - Sistemas periciales (INTCF, IMLs)
  - Registros administrativos de apoyo a la Administración de Justicia (SIRAJ)
  - Servicios de información a los órganos judiciales de datos necesarios en la tramitación judicial (PNJ)
  - Sistemas dirigidos a profesionales y a la ciudadanía: sedes judiciales electrónicas, LexNET, Acceda, etc.

[4] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2509-ccn-stic-803-valoracion-de-sistemas-en-el-ens-anexo-i-universidades/file.html

En relación con los sistemas denominados auxiliares, en términos generales, podría afirmarse que el origen o destino de la información que manejan es el expediente judicial o fiscal electrónico.

TRATAMIENTOS DE DATOS PERSONALES SOMETIDOS AL ENS

Los órganos jurisdiccionales, el Ministerio Fiscal, el Ministerio de Justicia y las Comunidades Autónomas están incluidos dentro de las entidades que, como responsables o encargados, deben aplicar las medidas de seguridad del ENS, de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[5].

Por su parte, Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, obliga a la aplicación del ENS en las medidas de seguridad[6].

La Agencia Española de Protección de Datos, en su Guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales[7], ha propuesto una correspondencia entre el nivel de riesgo para los derechos y libertades y las categorías del ENS:

Nivel de riesgo para los derechos y libertades	Categoría ENS
Muy Alto	Alto
Alto	Alto
Medio	Medio
Bajo	Bajo

La AEPD recopila en la citada guía una lista de **factores de riesgo** mínimos previstos en la normativa, que se derivan del tratamiento de los datos personales, para los derechos y libertades de los ciudadanos en particular, y de la sociedad en su conjunto, evaluando el nivel de riesgo, salvo en los efectos colaterales del tratamiento y brechas de datos personales sujetos a valoración de la probabilidad.

Operaciones relacionadas con los fines de tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.
Tipos de datos utilizados	Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

[5] Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.
2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado
[6] Artículo 37. Seguridad del tratamiento.
1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.
[7] https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Extensión y alcance del tratamiento	Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.
Categorías de interesados	Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.
Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.
Recogida y generación de datos	Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.
Efectos colaterales del tratamiento	Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Categoría del responsable/encargado	Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
Comunicaciones de datos	Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.
Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.

Asimismo, se recogen otros posibles, y no exhaustivos, factores de riesgo no previstos en la normativa.

Por último, se consideran **riesgos de muy alto impacto** para el caso de tratamientos en los que el compromiso de las garantías básicas de un Estado de Derecho pudiera verse afectado y tener un impacto de altísima repercusión a nivel social sobre los derechos y libertades de los ciudadanos, entre ellos los tratamientos de las AAPP, entidades de telecomunicaciones, financieras, aseguradores, proveedores de servicios de internet o Cloud, etc.

Como ejemplos de muy alto impacto indica los siguientes:

Factor de riesgo
Quiebras del Estado de Derecho
Alteración radical de las garantías jurídicas
Cambios geoestratégicos
Avances tecnológicos disruptivos
Situaciones de emergencia nacional
Otros

5. CRITERIOS DE VALORACIÓN

Los criterios generales y específicos en materia de protección de datos, indicados en los apartados anteriores son perfectamente aplicables en el ámbito de la Administración de Justicia, dado que los incidentes de seguridad en sus sistemas pueden afectar a la prestación normal del servicio público de justicia, a los derechos de los ciudadanos, a la reputación nacional e incluso internacional, en la cooperación jurídica internacional, pudiendo tener también impactos económicos.

En materia de derechos de las personas, y dado el presente ámbito sectorial, se destacan los derechos fundamentales recogidos en el artículo 24 de la Constitución Española, cuyo contenido se podría sintetizar en el derecho a la tutela judicial efectiva, a la prohibición de la indefensión, a las garantías constitucionales del proceso penal, a la presunción de inocencia y a la exclusión del deber de testificar[8].

Los escenarios potencialmente más graves, como la pérdida masiva de información o su exfiltración, podrían tener impacto en el propio Estado de Derecho.

Se consideran, a continuación, los criterios relativos al impacto en las personas, y el impacto legal.

5.1 El respeto de los derechos de las personas

Confidencialidad

Los datos contenidos en los sistemas de la Administración de Justicia son muy heterogéneos: contiene datos de carácter personal, categorías especiales de datos, datos de naturaleza penal, datos de infracciones y sanciones administrativas, datos de personas vulnerables como víctimas de delitos, menores y discapacitados.

Un incidente de seguridad sobre estos datos podría suponer una violación de los derechos de las personas, especialmente de sus derechos fundamentales, principalmente y sin perjuicio de otros:

- Derecho a la tutela judicial efectiva y a las garantías procesales
- Derecho al honor, a la intimidad personal y familiar y a la propia imagen
- Derecho a la protección de datos
- Derecho a la integridad física y moral
- Derecho a la libertad y seguridad
- Derecho al secreto de las comunicaciones

La pérdida de confidencialidad del contenido de actuaciones sometido a secreto, puede poner en riesgo la integridad y seguridad de una víctima de delito o de un testigo protegido, así como suponer un riesgo para el resultado de la investigación o del proceso, con la represión del delito en su caso.

[8] https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=24&tipo=2

Una violación de los datos constitutivos de secreto empresarial, en un proceso judicial, puede afectar muy gravemente al ámbito económico patrimonial de sus titulares.

Integridad

La pérdida de la integridad de los datos de los expedientes judiciales puede afectar de manera muy grave a los derechos de las personas, principalmente a su derecho a la tutela judicial efectiva, si los autos no pudieran reconstruirse, o si la modificación no autorizada de los documentos afecta a las personas o a las decisiones procesales.

Autenticidad

Las dimensiones de autenticidad y de trazabilidad están destinadas a la protección de las clásicas dimensiones de confidencialidad e integridad[9].

El acceso a los sistemas por las personas autorizadas (usuarios, profesionales, ciudadanos) ha de ser proporcional a la información y al servicio que se trata de proteger, o al acto procesal electrónico o telemático a realizar.

Trazabilidad

El simple acceso indebido ya supone una pérdida de confidencialidad de los datos personales y objeto de infracción administrativa, y disciplinaria.

Si el acceso indebido es a datos reservados de carácter personal o familiar, constituye un ilícito penal (art. 197.2 CP y 198 CP en caso de funcionarios púbicos), que es agravado en caso de acceso a categorías especiales de datos.

La incapacidad para rastrear un acceso a la información dificultaría e incluso podría imposibilitar conocer la identidad del autor del acceso ilícito, y en muchos casos, dada la información obrante en los expedientes judiciales o fiscales, constituiría la imposibilidad de perseguir delitos.

Disponibilidad

La falta de disponibilidad del sistema puede tener como consecuencia la dilación en la realización de los diferentes tramites de los procesos, con impacto en el derecho fundamental de los ciudadanos a la tutela judicial efectiva y un proceso sin dilaciones indebidas (extensible a todas las jurisdicciones). Este impacto se agrava por el elevado número de personas afectadas, y los plazos actuales de resoluciones de los expedientes judiciales pendientes.

En el caso de indisponibilidad de los Registros administrativos de apoyo a la Administración de Justicia, podría tener un elevado impacto en los derechos de las personas y en la seguridad pública, al no poder consultar y comprobar la peligrosidad

[9] MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I Método. (pág. 25). Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad y disponibilidad. En esta metodología se han añadido la autenticidad y el concepto de trazabilidad (del inglés, accountability), que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, etc.
https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

de un detenido e incluso la existencia de una medida cautelar, dejando en libertad a un sospechoso sobre el que recae una orden de búsqueda y captura.

5.2 Impacto legal

El impacto en los derechos y libertades de las personas constituye un incumplimiento del ordenamiento jurídico, salvo en aquellos incidentes que escapan a las razonables y proporcionales medidas de seguridad.

Un incidente de seguridad sobre los activos puede suponer el incumplimiento de una norma jurídica, particularmente aquellas normas que obligan a preservar las diferentes dimensiones de seguridad en las normas procesales, y en el marco normativo de protección de datos.

En el ámbito de la Administración de Justicia, existen normas dirigidas a respetar la confidencialidad de los datos, otras dirigidas a garantizar la autenticidad e integridad de los documentos procesales y de actuaciones procesales grabadas, así como la autenticidad e integridad de los documentos aportados por las partes y peritos.

En general, los sistemas puestos a disposición de la Administración de Justicia deben respetar, con su propio régimen especial, la normativa orgánica de protección de datos personales. Entre ellos, los sistemas que tramiten los procesos, los sistemas de comunicaciones con los profesionales y otros agentes, las sedes judiciales electrónicas, donde los ciudadanos pueden relacionarse con la Administración de Justicia mediante la realización de trámites de presentación de escritos, acceso a las notificaciones, estado de sus expedientes, entre otros.

El artículo 1.2 del Real Decreto-ley 6/2023, de 19 de diciembre, establece que "*En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en el presente real decreto-ley, asegurando la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación, portabilidad e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones.*"

Cuando valoramos un incidente de seguridad sobre algunas de las dimensiones, entendemos que el incidente supondría un incumplimiento normativo, principalmente de las normas que recogen lo arriba indicado:

- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Leyes procesales.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- 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.

Confidencialidad e integridad

Entendemos que los supuestos más probables se corresponderían con la pérdida de confidencialidad o integridad como consecuencia de una quiebra de seguridad de los sistemas. En estos supuestos, se podrían generar responsabilidades por la falta de medidas técnicas y organizativas apropiadas, para garantizar un nivel de seguridad adecuado al riesgo, e impedir un acceso no autorizado o la alteración de los datos.

Autenticidad

La autenticidad de los documentos y de las actuaciones de las oficinas y de los órganos judiciales y fiscales, la autenticación de los ciudadanos y profesionales, y de magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos, viene regulada en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales, el Real Decreto-ley 6/2023, de 19 de diciembre, y en su norma de desarrollo, el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET.

Trazabilidad

Esta incapacidad supone en sí misma la falta de adopción de medida de seguridad consistente en el registro de la actividad de los usuarios, medida para garantizar la confidencialidad e integridad evitando el acceso o uso indebido de la información.

La trazabilidad viene regulada en el Real Decreto-ley 6/2023, de 19 de diciembre, RGPD, Ley Orgánica 7/2021, ENS, EJIS.

Disponibilidad

Para cada sistema concreto se considerará la existencia de norma o legislación que establezca unas obligaciones específicas de disponibilidad.

Por ejemplo, para los actos de comunicación electrónica (Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET):

> *"Los medios electrónicos relacionados en los artículos anteriores estarán en funcionamiento durante las veinticuatro horas del día, todos los días del año".*

Asimismo, se considerarán las obligaciones de las Administraciones prestatarias de medios materiales de proveer los medios adecuados para el ejercicio de las funciones.

APLICABILIDAD DE LOS CRITERIOS DE VALORACIÓN

El escenario ideal para valorar el impacto serían los propios expedientes judiciales o fiscales, de manera individual. Sin embargo, poco sentido tendría si coexisten en el mismo sistema o base de datos necesariamente con otros expedientes de superior o inferior impacto.

Otra opción de valoración podría efectuarse por tipos de tramitación o procedimiento y jurisdicción, siempre que estén separados del resto de jurisdicciones. No obstante, entendemos que pueden existir impactos muy elevados, en general, en todas las jurisdicciones.

Con estas premisas, el sistema debe alcanzar la valoración de su máximo impacto, con la consecuente sobreprotección de determinados activos de menor valor.

En base a los criterios de valoración expuestos en el apartado anterior, se proponen las siguientes valoraciones mínimas para los sistemas de información en el ámbito de la Administración de Justicia, en función de aspectos tales como tipo de dato, sistema, procedimiento, posible impacto o riesgo en las personas:

DIMENSIÓN	BAJO	MEDIO	ALTO
C	**Impacto leve en los derechos de las personas** por la naturaleza de la información • Datos personales no constitutivos de categorías especiales, y no recogidos en los niveles superiores.	**Impacto grave** en los derechos de las personas por la naturaleza de la información • Datos personales de categoría especial • Datos económicos y tributarios • Datos de infracciones y sanciones administrativas	**Impacto muy grave** en los derechos de las personas por la naturaleza de la información • Datos de menores y personas vulnerables • Datos de víctimas de delito • Datos de testigos protegidos • Datos de naturaleza penal • Datos de procedimientos judiciales de menores • Datos personales, incluidos los de categoría especial, que puedan afectar a la intimidad personal o familiar, honor e imagen. **Impacto muy grave en la consecución de las finalidades** • Datos objeto de secreto de sumario • Datos objeto de secreto empresarial

DIMENSIÓN	BAJO	MEDIO	ALTO
I	Datos reintegrables fácilmente -por obrar en otros sistemas de información-	Datos reintegrables con perjuicios en los derechos de las personas – p.ej. Derecho a un proceso sin dilaciones indebidas. Información que puede ser reconstruida – p.ej. Procedimiento de reconstrucción de autos.	Datos no reintegrables con graves perjuicios en los derechos de las personas -p.ej. Tutela judicial efectiva-, o que pueden afectar a la consecución de las propias finalidades del proceso. P.ej. Sistemas de grabación- pérdida o destrucción de grabaciones, documentos judiciales electrónicos que no puedan ser reconstruidos, suponen la nulidad de la actuación procesal, con imposibilidad de repetición de la vista, declaraciones.
A		El nivel medio de autenticidad puede venir determinado: -Por la naturaleza de la información tratada y servicios prestados -Sistemas que no se relacionan con los ciudadanos o profesionales.	El nivel alto de autenticidad puede venir determinado: -Por la naturaleza de la información tratada y servicios prestados -Por la necesidad de garantizar la identificación de los interesados y profesionales en la realización de los trámites y actos procesales -Por la necesidad de garantizar la autenticidad y no repudio de los documentos aportados.
T		Sistemas que contengan información, o presten servicios, cuya vulneración tenga un impacto grave en los derechos de los ciudadanos, y las acciones puedan ser constitutivas de infracciones administrativas graves o muy graves en materia de protección de datos personales o de delitos.	Sistemas, que, por la naturaleza y sensibilidad de la información tratada y la importancia de los servicios prestados, particularmente en los derechos y libertades, requieren de los máximos controles de trazabilidad para prevenir y perseguir la comisión de violaciones que pudieran ser constitutivas de delitos. Principalmente aquellos sistemas que contienen información cuya vulneración afectaría muy gravemente a los derechos de sus titulares o a la consecución de las finalidades principales.

DIMENSIÓN	BAJO	MEDIO	ALTO
			Entre estos sistemas se incluyen los del ámbito de la Ley Orgánica 7/2021.
D	Se puede realizar o continuar el trámite por otro medio	-Se dificulta la capacidad de usuarios o ciudadanos para la realización del trámite -Se dificulta o se reduce significativamente la capacidad del organismo para ejecutar las funciones principales (el impacto es recuperable) -Existe normativa o ANS con tercero que justifique RTO menor de 24h	-Se anula la capacidad del organismo para ejecutar las funciones principales, o el servicio principal motivado por la falta de disponibilidad del sistema analizado. -La indisponibilidad del sistema podría tener un elevado impacto en los derechos de las personas – p.ej. Sistema de registros administrativos de apoyo a la Administración de Justicia, al no poder consultar y comprobar la peligrosidad de un detenido, la existencia de una medida cautelar, o de una requisitoria cuyo conocimiento hubiera facilitado la detención, y evitado los riesgos para los derechos de los ciudadanos. -Existe normativa o ANS con tercero que justifique RTO menor de 4h