Temario de Normativa General FISIOTERAPIA

IL·LUSTRE COL·LEGI OFICIAL DE FISIOTERAPEUTES DE LA COMUNITAT VALENCIANA

TEMA 4

PRNCIPIOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. CERTIFICADOS Y FIRMA ELECTRÓNICOS. USO SEGURO DE MEDIOS TECNOLÓGICOS

Autora
Silvia Caplliure Fauri
Abogado Asesoría Jurídica SATSE Valencia.

Índice

Tema 4

Principios básicos de la seguridad de la información. Protección de datos de carácter personal. Certificados y firma electrónicos. Uso seguro de medios tecnológicos

1. Los principios básicos de la seguridad de la información 5
2. La protección de datos de carácter personal 6
2.1. Definiciones 6
2.2. Principios 9
2.3. Consentimiento otorgado para el tratamiento de datos personales 10
2.4. Derechos de los interesados 10
2.5. Tratamiento de datos personales 12
3. Uso seguro de medios tecnológicos 13
3.1. Objeto 13
3.2. Ámbito de aplicación 13
3.3. Principio general de actuación 14
3.4. Definiciones 14
3.5. Propiedad y uso de los medios tecnológicos 15
3.6. Identificación de acceso 15
3.7. Copias de seguridad 16
3.8. Notificación de incidencias 16
3.9. Inspección de los medios tecnológicos 16
3.10. Cese de actividad 16
3.11. Correo electrónico corporativo 16
3.12. Acceso a internet desde la RCGVA 17
3.13. Incumplimientos 17
4. Certificados electrónicos y firma electrónica 18
4.1. Origen 18
4.2. Objeto y ámbito de aplicación 18

4.3. El documento nacional de identidad y sus certificados electrónicos 18
4.3.1. Efectos jurídicos de los documentos electrónicos 19
4.3.2. Vigencia y caducidad de los certificados electrónicos 19
4.3.3. Revocación y suspensión de los certificados 20
4.3.4. Identidad de los sujetos titulares de los certificados electrónicos 20
4.3.5. Los prestadores de servicios electrónicos de confianza 21
4.4. Certificados electrónicos de confianza no cualificados 22
4.5. Obligaciones de seguridad y control 22
4.6. Supervisión y control 23
4.7. Infracciones y sanciones 23
5. Referencias legislativas 26

1. Los principios básicos de la seguridad de la información

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se regulan en la Orden JUS/1293/2017, de 14 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica. Se establecen los siguientes:

Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada, el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados, el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

2. La protección de datos de carácter personal

La protección de las personas físicas en relación con el tratamiento de los datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución Española. De esta forma nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La protección de datos de carácter personal se encuentra regulada mediante el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y posteriormente fue adaptada al ordenamiento jurídico español en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mediante La ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.1. Definiciones

En el artículo 4 del Reglamento (UE) 2016/679 enumera las siguientes definiciones:

> **Datos personales**: Toda información sobre una persona física identificada o identificable (el interesado): Se considerara persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Limitación del tratamiento: El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Seudonimizacion: El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y este sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Fichero: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Responsable del tratamiento o responsable: La persona física o jurídica, autori-

dad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Encargado del tratamiento o encargado: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Destinatario: La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Tercero: Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Consentimiento del interesado: Es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Violación de la seguridad de los datos personales: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Datos genéticos: Son los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos biométricos: Son los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos relativos a la salud: Son los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Establecimiento principal

Por un lado, en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerara establecimiento principal;

Por otro lado, en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encarga-

do en la medida en que el encargado este sujeto a obligaciones especificas con arreglo al presente Reglamento.

Representante: Es la persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.

Empresa: Se considera una empresa a la persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

Grupo empresarial: Grupo constituido por una empresa que ejerce el control y sus empresas controladas.

Normas corporativas vinculantes: Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Autoridad de control: La autoridad pública independiente establecida por un Estado miembro.

Autoridad de control interesada: La autoridad de control a la que afecta el tratamiento de datos personales debido a que:

- El responsable o el encargado del tratamiento esta establecido en el territorio del Estado miembro de esa autoridad de control.
- Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o se ha presentado una reclamación ante esa autoridad de control.

Tratamiento transfronterizo: El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado esta establecido en más de un Estado miembro, o el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Objeción pertinente y motivada: La objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

Servicio de la sociedad de la información: Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

Organización internacional: Una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

2.2. Principios

Con el objetivo de garantizar una protección mayor de los datos de carácter personal de los ciudadanos de la Unión Europea, el RGDPD establece los siguientes principios comunes a todos los estados miembros:

Principio de licitud, lealtad y transparencia

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- El interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
- El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Principio de limitación de la finalidad

Los datos personales serán recabados con una finalidad determinada, de forma explicita y legitima, y no serán tratados ulteriormente de manera incompatible con dichos fines, salvo que sean destinados a fines de archivo en interés público, fines de investigación científica e historia o fines estadísticos.

Principio de exactitud

Los datos personales habrán de ser exactos y cuando sea necesario habrán de actualizarse, adoptando todas las medidas que se consideren necesarias para que se supriman o rectifiquen ciertos datos personales que resulten inexactos o erróneos para los fines que se recabaron.

Principio de minimización de datos

Los datos personales habrán de ser adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados.

Principio de limitación del plazo de conservación

El principio de limitación del plazo de conservación, esta relacionado con el de minimización, ya que solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad. Y la conservación de estos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Alcanzados los fines previstos, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

Principio de integridad y confidencialidad

El principio de integridad y confidencialidad impone a quienes tratan los datos personales, la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

2.3. Consentimiento otorgado para el tratamiento de datos personales

Conviene resaltar que por consentimiento del interesado , se entiende toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. Siendo nulo el consentimiento para la comunicación de datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentara de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectara a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Sera tan fácil retirar el consentimiento como darlo.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

2.4. Derechos de los interesados

Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

Derecho de acceso

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

- Los fines del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales.

- De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Derecho de rectificación

El Derecho de rectificación consiste en que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Derecho de supresión

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

- Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- El interesado retire el consentimiento en que se basa el tratamiento.
- El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento.
- Los datos personales hayan sido tratados ilícitamente.
- Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información

Derecho a la limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- El interesado se haya opuesto al tratamiento.

Derecho a la portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento

sin que lo impida el responsable al que se los hubiera facilitado, cuando el tratamiento este basado en el consentimiento o se efectué por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

Derecho de oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento.

El responsable del tratamiento dejara de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que este relacionada con la citada mercadotecnia.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

2.5. Tratamiento de datos personales

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informara al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulara, en particular, que el encargado:

> Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que este obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado y en tal caso, el encargado informara al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
>
> Garantizara que las personas autorizadas para tratar datos personales se hayan com-

prometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

Tomará todas las medidas necesarias.

Respetará las condiciones indicadas para recurrir a otro encargado del tratamiento.

Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.

Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realizacion de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

Cuando un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

3. Uso seguro de medios tecnológicos

El uso de medios tecnológicos se encuentra regulado en la Orden 19/2013 de la Conselleria de Hacienda y Administración Pública, por la que se establecen las normas sobre el uso seguro de medios tecnológicos en la administración de la Generalitat Valenciana.

3.1. Objeto

Esta orden presenta como objetivo minimizar las amenazas que puedan suponer un riesgo en los sistemas de información de la Generalitat, estableciendo una serie de normas que tendrán que cumplir todos los usuarios de los medios tecnológicos de la Administración de la Generalitat.

3.2. Ámbito de aplicación

Será considerado usuario cualquier persona que utilice o tenga acceso a los medios tecnológicos puestos a su disposición por la Administración de la Generalitat.

Los contenidos desarrollados en la Orden 19/2013, de 3 de diciembre, de la Conselleria de Hacienda y Administración Pública, por la que se establece las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat Valenciana, serán de obligatorio cumplimiento para todos los usuarios y sus contenidos desarrollan las directrices de carácter general que se definen en la política de seguridad de la información.

3.3. Principio general de actuación

Todos los usuarios de los medios tecnológicos de la Administración de la Genalitat Valenciana se comprometen a hacer un uso correcto de todos los elementos que requieran para el desarrollo de sus funciones, a respetar las medidas de seguridad que se establezcan y a comunicar si detectasen algún punto débil en la seguridad de estos.

3.4. Definiciones

El artículo 4 de la Orden 19/2013, hace referencia a que han de ser comprendidos una serie de conceptos relativos a la protección de datos de carácter personal, que se detallan en el Anexo I de la citada Orden, siendo los siguientes:

Amenaza: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Contraseña o clave de acceso: Información secreta, en general compuesta por un grupo de caracteres, utilizada para la autenticación.

Copia de seguridad o respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Dispositivos móviles: Un dispositivo móvil se puede definir como un equipo de un tamaño pequeño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

Cifrado: Transformación criptográfica de datos para producir un criptograma o texto cifrado.

Equipo portátil: Es aquel ordenador personal que es capaz de realizar la mayor parte de las tareas que realizan los ordenadores de sobremesa, con similar capacidad, con la ventaja de su peso y tamaño reducidos, así como su movilidad.

Identificación de acceso: Proceso que limita y controla el acceso a los recursos de un sistema de información.

Información sensible: Aquella, así definida por su propietario, que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o a algo.

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Ordenadores personales: Son los equipos informáticos básicos de los puestos de trabajo donde estarán instaladas las aplicaciones necesarias para el desempeño de las funciones y desde los que accederá el usuario a la red corporativa y a los sistemas de información.

Perfil: Limitación del acceso a los recursos exclusivamente a personas, entidades o a procesos con la debida autorización.

Telefonía fija: Es aquella que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales

telefónicos no portables, y generalmente enlazados entre ellos o con la central por medio de conductores metálicos.

Red Corporativa de la Generalitat Valenciana (RCGVA): Es la infraestructura común para la interconexión de las sedes de todas las conselleríias y organismos, tanto a nivel de los servicios de datos como de voz, con distribución geográfica que abarca toda la Comunitat Valenciana.

Red informática: Sistema de comunicación que conecta ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos.

Red inalámbrica: La conexión de equipos por medios de ondas electromagnéticas y sin necesidad de una conexión física mediante cables. Las redes más usuales suelen ser Wifi, Bluetoohth, o infrarrojos.

3.5. Propiedad y uso de los medios tecnológicos

Son propiedad de la Administración de la Generalitat, el conjunto de todos los medios tecnológicos puestos a disposición de los usuarios como son ordenadores personales y portátiles, aplicaciones, programas, sistemas de impresión y escaneo de documentos, dispositivos móviles, el acceso a la red corporativa y a internet.

La Administración de la Generalitat le facilitará a cada usuario un lugar de trabajo con los medios tecnológicos necesarios para el desempeño de las funciones encomendadas. Estos medios no están pensados para al uso personal, y no podrán utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento de la Administración de la Generalitat o sean contrarias a los intereses de esta.

Alterar sin la debida autorización, cualquiera de los componentes físicos o lógicos de los medios tecnológicos, estará prohibido salvo autorización expresa del organismo con competencias en tecnologías de la información. En todo caso, estas operaciones solo podrán realizarse por el personal de soporte técnico autorizado.

Para la instalación, utilización o conexión a la red corporativa de cualquier medio tecnológico ajeno, se requerirá de una autorización previa por parte del órgano competente en materia de tecnologías de la información que corresponda. Estando estrictamente prohibida la ejecución de programas informáticos en los medios tecnológicos que forman parte de los sistemas de información de la Administración de la Generalitat sin la correspondiente licencia de uso y autorización correspondiente del organismo con competencias en tecnologías de la información.

Toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas, estará terminantemente prohibida.

3.6. Identificación de acceso

La identificación de acceso a cualquier medio tecnológico deberá de ser personal e intransferible.

Los usuarios serán los responsables de toda la actividad relacionada con el uso de su acceso personal autorizado, deberán custodiar su identificación de acceso y en ningún caso podrá ser suministrada a terceras personas.

Cuando un usuario tenga sospechas de que su identificación de acceso está siendo utilizada por un tercero, deberá comunicar inmediatamente al organismo con competencias en tecnologías de la información la correspondiente incidencia de seguridad.

Los usuarios deben utilizar contraseñas seguras de acuerdo con la política de contraseñas definida por el órgano con competencias en materia de tecnologías de la información.

3.7. Copias de seguridad

La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad del órgano competente en materia de tecnologías de la información. Cada usuario será responsable de la integridad y copia de seguridad de la información almacenada en el medio tecnológico que tenga asignado.

3.8. Notificación de incidencias

Una incidencia de seguridad en un sistema, la constituye cualquier situación o eventualidad en la que pueda verse amenazada la información, y pueda en consecuencia dar lugar a una pérdida de: confidencialidad, integridad, disponibilidad y autenticidad.

Todos los usuarios están obligados a notificar cualquier incidencia de seguridad a través del procedimiento establecido a tal efecto.

3.9. Inspección de los medios tecnológicos

El órgano competente en materia de tecnologías de la información establecerá por razones específicas de seguridad o de evaluación del desempeño, medidas de control y comprobará mediante los mecanismos formales y técnicos que estime oportunos, la correcta utilización por parte de los usuarios de todos los medios tecnológicos puestos a su disposición para el desempeño de sus funciones. Estos controles y revisiones se realizarán respetando los principios de necesidad, idoneidad y proporcionalidad, preservando las garantías del derecho a la intimidad del usuario y la seguridad de las comunicaciones.

3.10. Cese de actividad

El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al organismo con competencias en tecnologías de la información.

Cuando se modifiquen las circunstancias profesionales que originaron la entrega de un medio tecnológico, el usuario lo devolverá al organismo con competencias en tecnologías de la información, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

3.11. Correo electrónico corporativo

Las cuentas creadas en los servidores de la Administración de la Generalitat tienen como objetivo el intercambio de mensajes propios del desempeño profesional. Queda prohibido su uso con fines comerciales, financieros o personales.

No están permitidos los envíos masivos, siendo rechazados los mensajes si el número máximo de destinatarios es superior al límite establecido por el órgano con competencias en materia de tecnologías de la información.

No se debe utilizar el correo para anunciar la aparición de nuevos virus, amenazas, etc. Queda totalmente prohibido suplantar la identidad de una persona a través del correo electrónico. No se permite el uso de cuentas de correo distintas a las proporcionadas por la Administración de la Generalitat dentro de la RCGVA, salvo autorización expresa del órgano con competencias en materia de tecnologías de la Información. Los usuarios no deben enviar mensajes con información sensible tanto en el cuerpo del mensaje como en los archivos adjuntos. Este envío únicamente

podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información sea inteligible o manipulada por terceros (cifrado y firma electrónica).

El correo electrónico es una de las fuentes más importantes de difusión de virus por lo que se recomienda no abrir mensajes recibidos de remitentes desconocidos y para garantizar la identidad del remitente los correos se firmarán electrónicamente.

Debido al incremento y a la continua aparición de nuevos virus, se eliminarán automáticamente los mensajes con anexos susceptibles de ejecución, y se limitará el tamaño máximo de los ficheros adjuntos y se asignará a los usuarios un tamaño máximo de buzón.

3.12. Acceso a internet desde la RCGVA

El acceso a internet desde la RCGVA se encuentra supeditado a las siguientes condiciones de acceso:

El acceso a internet se realizará únicamente a través de la salida a internet establecida por el órgano con competencias en materia de tecnologías de la información utilizando los medios tecnológicos que se dispongan a tal fin.

El acceso a internet por otros medios, está expresamente prohibido.

Los recursos de internet serán filtrados según su contenido a través de sistemas automatizados y cada usuario tendrá asignado un perfil de acceso en función de su puesto de trabajo, que determinará a qué tipo de contenidos podrá acceder y en que horarios.

Los perfiles de acceso serán creados por el órgano con competencias en materia de tecnologías de la información.

La responsabilidad del usuario final se concreta en los siguientes extremos:

La utilización de internet debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse toda utilización que no tenga una mínima relación con las funciones encomendadas al usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado.

No está permitido el acceso a páginas de contenido ofensivo, inapropiado, pornográfico, o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social.

No se permite la descarga desde internet de cualquier clase de programas, aplicaciones, documentos o archivos que no provengan de páginas oficiales relacionadas con el trabajo, todo ello con la finalidad de que la descarga no pueda poner en peligro los sistemas informáticos y la información que la Generalitat custodia.

3.13. Incumplimientos

El incumplimiento de las normas de uso expresadas en esta orden podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

4. Certificados electrónicos y firma electrónica

Los certificados electrónicos y firma electrónica se encuentran regulados en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.1. Origen

El 1 de julio de 2016 entró en vigor el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado anterior y por el que se derogo la Directiva 1993/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, supuso la transposición al ordenamiento jurídico español de la derogada Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se estableció un marco comunitario para la firma electrónica, encontrándose desde entonces jurídicamente desplazada en todo aquello regulado por el citado Reglamento

La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza deroga la Ley 59/2003, de 19 de diciembre, de firma electrónica y complementa algunos preceptos regulados en el Reglamento (UE) ella aquellos preceptos incompatibles con el Reglamento (UE) 910/2014.

4.2. Objeto y ámbito de aplicación

La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

El objeto de esta Ley es, por tanto, adaptar nuestro ordenamiento jurídico al marco regulatorio de la Unión Europea, evitando así la existencia de vacíos normativos susceptibles de dar lugar a situaciones de inseguridad jurídica en la prestación de servicios electrónicos de confianza.

La función de esta Ley es complementarlo en aquellos aspectos concretos que el Reglamento UE 910/2014, no ha armonizado y cuyo desarrollo prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España.

Es por ello que se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.

4.3. El documento nacional de identidad y sus certificados electrónicos

El Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar electrónicamente la identidad personal de su titular, así como la firma electrónica de documentos.

Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los

documentos firmados con sus certificados electrónicos.

Los órganos competentes del Ministerio del Interior para la expedición del Documento Nacional de Identidad cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados.

Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se regirá por su normativa específica.

Hasta que se desarrolle reglamentariamente el Documento Nacional de Identidad, se mantendrá en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Un certificado electrónico emitido y firmado por una entidad con capacidad para ello, sirve para identificar a una persona.

A la entidad en cuestión se le suele denominar como autoridad de certificación o prestador de servicios de certificación. Tal documento, identifica a una persona física o jurídica y a una clave pública que se le ha asignado para poder realizar procesos de firma y/o cifrado. Cada certificado está identificado por un número de serie único y tiene un período de validez que está incluido en el certificado.

4.3.1. Efectos jurídicos de los documentos electrónicos

Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto.

" Artículo 326. Fuerza probatorio de los documentos privados

(...)

3. *Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.*
4. *Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados."*

4.3.2. Vigencia y caducidad de los certificados electrónicos

Los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.

El período de vigencia de los certificados cualificados no será superior a cinco años.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

4.3.3. Revocación y suspensión de los certificados

Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:

Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.

Resolución judicial o administrativa que lo ordene.

Fallecimiento del firmante, capacidad modificada judicialmente sobrevenida, total o parcial, del firmante, extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.

Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.

Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

El prestador de servicios electrónicos de confianza comunicará de manera previa o simultanea al titular, por un medio que acredite la entrega y recepción efectiva siempre que sea factible, la revocación o suspensión del certificado electrónico siempre, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

En los casos de suspensión, la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

4.3.4. Identidad de los sujetos titulares de los certificados electrónicos

La identidad de los sujetos titulares de los certificados electrónicos esta regulada en los Artículos 6 y 7 de la Orden 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.

El artículo 6 determina de que forma han de autentificarse en los certificados cualificados las personas físicas, jurídicas y sus representantes. Debiendo realizarlo de la siguiente forma :

En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.

En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

Y en el caso de que los certificados admitan una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

En cuanto a la regulación de la comprobación de la identidad de los sujetos propietarios de los certificados, se estará a la identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, estas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica. Y serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

4.3.5. Los prestadores de servicios electrónicos de confianza

Los prestadores de servicios electrónicos de confianza cuentan con las siguientes obligaciones:

Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible.

Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

En cuanto a las responsabilidad los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si han actuado con la debida diligencia.

El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

Tampoco resultará responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

4.4. Certificados electrónicos de confianza no cualificados

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

4.5. Obligaciones de seguridad y control

Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

Tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten. Y ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

4.6. Supervisión y control

El Ministerio de Asuntos Económicos y Transformación Digital, como órgano de supervisión, controlará el cumplimiento por los prestadores de servicios electrónicos de confianza cualificados y no cualificados que ofrezcan sus servicios al público de las obligaciones establecidas en el Reglamento (UE) 910/2014 y en esta Ley.

En particular, podrá dictar directrices para la elaboración y comunicación de informes y documentos, así como recomendaciones para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los servicios de confianza, así como sobre requisitos y normas técnicas de auditoría y certificación para la evaluación de la conformidad de los prestadores cualificados de servicios de confianza

El Ministerio de Asuntos Económicos y Transformación Digital realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control. Los funcionarios adscritos al Ministerio de Asuntos Económicos y Transformación Digital que realicen la inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

El plazo máximo para dictar y notificar resolución en el procedimiento de verificación previa de cumplimiento de los requisitos establecidos en el citado Reglamento será de 6 meses, transcurridos los cuales se podrá entender desestimada la solicitud.

La revocación de la cualificación a un prestador o a un servicio mediante su retirada de la lista de confianza es independiente de la aplicación del régimen sancionador.

En cuanto a la información y colaboración los prestadores de servicios de confianza, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios de confianza, tienen la obligación de facilitar al Ministerio de Asuntos Económicos y Transformación Digital toda la información y colaboración precisas para el ejercicio de sus funciones.

Si el organismo de certificación perteneciera a la Autoridad Nacional de Certificación de la Ciberseguridad o estuviese supervisado por ella, se acordarán con dicha Autoridad los mecanismos de colaboración y el contenido de la información necesaria.

4.7. Infracciones y sanciones

Las infracciones se clasifican en muy graves, graves y leves:

Serán consideradas como infracciones **muy graves**:

- La comisión de una infracción grave en el plazo de dos años desde que hubiese sido sancionado por una infracción grave de la misma naturaleza, contados desde que recaiga la resolución sancionadora firme.
- La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en el año anterior al inicio

del procedimiento sancionador o desde el inicio de la actividad del prestador si este periodo es menor.

Son infracciones **graves:**

- La resistencia, obstrucción, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.
- Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.
- En caso de que el prestador expida certificados electrónicos, almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.
- No proteger adecuadamente los datos de creación de firma, sello o autenticación de un sitio web
- No registrar o conservar la información a la que se refiere el artículo 9.3.a) de esta Ley.
- El incumplimiento de la obligación de notificación de incidentes.
- La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre.
- La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de diez días desde que aquellos se hubieren producido.
- El incumplimiento de las resoluciones dictadas por el Ministerio de Asuntos Económicos y Transformación Digital para requerir a un prestador de servicios de confianza que corrija cualquier incumplimiento de los requisitos establecidos en esta Ley y en el Reglamento (UE) 910/2014.
- La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control, a partir del segundo requerimiento.
- No cumplir con las obligaciones de constatar la verdadera identidad del titular de un certificado electrónico y de conservar la documentación que la acredite, en caso de consignación de un pseudónimo.
- El incumplimiento por parte de los prestadores cualificados y no cualificados de servicios de confianza de la obligación de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que presten.
- No extinguir la vigencia de los certificados electrónicos en los supuestos señalados en esta Ley.
- La prestación de servicios cualificados careciendo del correspondiente seguro obligatorio.

Serán consideradas infracciones **leves:**

- Publicar información no veraz o no acorde con esta Ley y el Reglamento (UE) 910/2014.
- No comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados cumpliendo con los plazos establecidos.
- El incumplimiento por parte de los prestadores cualificados de servicios

de confianza del deber de informar al organismos de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados y de su intención de cesar tales actividades

- El incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Asuntos Económicos y Transformación Digital antes del 1 de febrero de cada año.
- El incumplimiento del deber de comunicación del prestador cualificado del cese de la actividad a sus clientes a los que preste servicios y al órgano de supervisión con un antelación mínima de dos meses.
- La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control.

La sanciones se encuentran reguladas en el artículo 19 de la Ley 6/2020 y recoge las sanciones que se le impondrán al infractor en los siguientes casos:

Multa por importe de 150.001 hasta 300.000 euros por la comisión de infracciones muy graves.

Multa por importe de 50.001 hasta 150.000 euros por la comisión de infracciones graves.

Multa por importe de hasta 50.000 euros por la comisión de infracciones leves.

Se determinará la cuantía de las sanciones con aplicación de una graduación de importe mínimo, medio y máximo a cada nivel de infracción, teniendo en cuenta lo siguiente:

El grado de culpabilidad o la existencia de intencionalidad.

La continuidad o persistencia en la conducta infractora.

La naturaleza y cuantía de los perjuicios causados.

La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

El volumen de facturación del prestador responsable.

El número de personas afectadas por la infracción.

La gravedad del riesgo generado por la conducta.

Las acciones realizadas por el prestador encaminadas a paliar los efectos o consecuencias de la infracción.

Las resoluciones sancionadoras por la comisión de infracciones muy graves serán publicadas en el sitio de Internet del Ministro de Asuntos Económicos y Transformación Digital, con indicación, en su caso, de los recursos interpuestos contra ellas.

La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

5. Referencias legislativas

Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se Deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Constitución Española (BOE núm. 311, de 29 de diciembre de 1978)

La ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Orden 19/2013 de la Conselleria de Hacienda y Administración Pública, por la que se establecen las normas sobre el uso seguro de medios tecnológicos en la administración de la Generalitat Valenciana.

Orden JUS/1293/2017, de 14 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica.