Directrices para la asignación de niveles de seguridad en la identificación

Plataforma de Identificación, Autenticación y Firma

Fecha: 9 de Septiembre de 2015

Versión: 2.0

INDICE

1. INTRODUCCION

Los cambios sociales y la evolución tecnológica, así como las experiencias previas, hacen necesario actualizar la forma en la que los ciudadanos se identifican y firman trámites administrativos, en el ámbito de la administración electrónica. La normativa principal que regula este tipo de cuestiones va camino de los 10 años, y los cambios en este tiempo han sido sustanciales, con un aumento significativo de la banda ancha, de tecnologías móviles, de relaciones electrónicas de los ciudadanos continuas y generales con el sector privado, a modo de ejemplo, se puede ver el tremendo auge de la banca electrónica.

La administración pública no ha estado inactiva, y fruto de esos esfuerzos es el sistema cl@ve, con el que se pretende una adaptación a las nuevas realidades sociales, de relación con los ciudadanos, así como un cumplimiento de la normativa, después de la publicación del nuevo reglamento europeo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (http://www.boe.es/doue/2014/257/L00073-00114.pdf)

De esta forma, se amplían los métodos por el que el ciudadano se relaciona electrónicamente, con nuevas formas adaptadas a las nuevas realidades, consagrando el principio de que es el propio ciudadano el que elige el método de acuerdo a sus preferencias.

Se mantiene por tanto la posibilidad de relacionarse a través de los certificados clásicos, bien instalados en un equipo informático, bien a través de tarjetas criptográficas. Pero se amplían los métodos de identificación y firma, creándose el sistema de certificados electrónicos en la nube, y nuevos métodos de firma, basados en claves concertadas y enviadas al dispositivo móvil, que facilitan de manera significativa la identificación y la firma. También se hace obligatorio el reconocimiento transfronterizo, es decir, un estado miembro debe reconocer los métodos de identificación y firma del resto de estados, que cumplan con los requisitos establecidos en el Reglamento eIDAS.

Todo ello está incluido en el sistema cl@ve, a través de sus distintas modalidades, cl@ve Pin, cl@ve Permanente, certificados y conexión con otros estados miembros. Y es por ello por lo que todos los trámites de las AAPP deben estar integrados con este sistema, para poder tanto adaptarnos a la normativa europea, como a las nuevas demandas de los ciudadanos.

No todos los métodos de identificación y firma tienen el mismo nivel de seguridad. El Proyecto de Ley (actualmente en tramitación en el Congreso de los Diputados) del Procedimiento Administrativo Común de las Administraciones Públicas tiene en cuenta esta circunstancia[1]:

[1] *Artículo 11. Uso de medios de identificación y firma en el procedimiento administrativo.*
1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.
2. Las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:
a) Formular solicitudes.
b) Presentar declaraciones responsables o comunicaciones.
c) Interponer recursos.
d) Desistir de acciones
e) Renunciar a derechos.

2. ¿CUAL ES EL OBJETIVO DE ESTE DOCUMENTO?

El sistema Cl@ve permite al proveedor del servicio que se integra con el mismo seleccionar el nivel de seguridad requerido en la identificación electrónica de un ciudadano para el acceso a un procedimiento o servicio electrónico que las AAPP pongan a su disposición.

Este documento recoge la recopilación de la normativa que afecta al desarrollo del sistema Cl@ve, y, establece criterios y recomendaciones para facilitar la asignación del nivel de seguridad en la identificación electrónica.

La clasificación de los sistemas de identificación electrónica en función de su seguridad está regulada por el *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 la que se deroga la Directiva 1999/93/CE* (en adelante, Reglamento eIDAS)[2], que a su vez basa los criterios de clasificación en el modelo de QAA (*Quality of Authentication Assurance*) utilizado en el proyecto STORK[3] y en la norma ISO 29115.

Aunque el ámbito de aplicación del Reglamento eIDAS se limita a la identificación electrónica en el acceso transfronterizo a servicios públicos, el diseño del sistema Cl@ve se ha realizado de forma coherente con los niveles de seguridad definidos en el Reglamento, de manera que dichos niveles puedan equipararse a los niveles de aplicación en el acceso electrónico a servicios públicos en el interior del Estado español. Con ello se busca un alineamiento entre la identificación a nivel nacional y transfronterizo que simplifique tanto el mantenimiento de los sistemas de información que dan soporte a estos servicios como el uso de los mismos por los ciudadanos, y facilite el cumplimiento de las obligaciones establecidas en el Reglamento eIDAS.

---

[2] Accesible en el siguiente enlace: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910&qid=1429022140671

[3] El modelo QAA de STORK se puede consultar en el siguiente enlace: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

No obstante, la definición de los niveles de seguridad que establece el Reglamento Europeo eIDAS es muy general, lo que hace difícil su aplicación de manera homogénea, como esquema de referencia, a los servicios concretos que van a utilizar el sistema Cl@ve. Por ello, en este documento, se establecen unos criterios y se dan unas recomendaciones que permitan, a los servicios y procedimientos integrados con el sistema Cl@ve, asignar el nivel de seguridad en la identificación electrónica adecuado a los requerimientos de seguridad del servicio o procedimiento al que se acceda.

En todo caso deberá aplicarse el principio de proporcionalidad (que ya consagrara la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*) *"en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones"*.

3. NORMATIVA DE REFERENCIA

3.1. 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, (EN ADELANTE EIDAS).

El Artículo 8 del Reglamento europeo define tres niveles de seguridad de los sistemas de identificación electrónica: bajo, sustancial y alto. Estos niveles cumplirán los siguientes criterios:

1. el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;
2. el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;
3. el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad.

3.2. REAL DECRETO 3/2010, DE 8 DE ENERO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

El Esquema Nacional de Seguridad (en adelante ENS), regulado por el Real Decreto 3/2010, de 8 de enero, constituye el marco legal que permite definir y establecer las medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El ENS establece la necesidad de categorizar los sistemas de información, siendo la categoría de un sistema de información, en materia de seguridad, la que permitirá modular el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad:

1. Disponibilidad [D]. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
2. Autenticidad [A]. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
3. Integridad [I]. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
4. Confidencialidad [C]. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
5. Trazabilidad [T]. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

El proceso de categorización de un sistema de información consiste en identificar los activos de información que constituyen el sistema y evaluar el impacto que sobre la organización tendría la materialización de un riesgo que comprometiera alguna de las dimensiones de seguridad mencionadas.

El ENS recomienda utilizar tres niveles (BAJO, MEDIO Y ALTO) para categorizar el impacto de un incidente de seguridad referido a cada una de las dimensiones de seguridad, siendo la categoría del sistema el nivel más alto de todas las dimensiones.

1. Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio limitado:
    a. El sufrimiento de un daño menor por los activos de la organización.
    b. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
    c. Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
    d. Otros de naturaleza análoga.
2. Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio grave:
    a. El sufrimiento de un daño significativo por los activos de la organización.
    b. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
    c. Causar un perjuicio significativo a algún individuo, de difícil reparación.
    d. Otros de naturaleza análoga.

3. Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio muy grave:

    a. El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

    b. El incumplimiento grave de alguna ley o regulación.

    c. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

    d. Otros de naturaleza análoga.

3.3. REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE, POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece las medidas de seguridad que se deben aplicar a los ficheros que contengan datos de carácter personal, tanto automatizados como no automatizados, y a su tratamiento.

Así, en su artículo 80 señala que *"Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.",* mientras que en su artículo 81 se especifica en qué circunstancias, atendiendo a la naturaleza de los datos tratados o mantenidos en esos ficheros, se deben aplicar las medidas de seguridad de cada nivel.

En cuanto a las medidas en sí, se detallan en el Capítulo III, e incluyen, en los ficheros y tratamientos automatizados, medidas relativas a la identificación y la autenticación, funciones objeto del sistema Cl@ve.

En particular, en el artículo 93 se establecen las siguientes medidas de seguridad para todos los niveles:

1. *El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.*
2. *El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.*
3. *Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.*
4. *El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.*

En el artículo 98 se establece la siguiente medida adicional para el nivel medio:

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Y no se exigen medidas adicionales para el nivel alto, si bien se exigen en el artículo 103 controles especiales de registro de acceso.

4. NIVELES DE SEGURIDAD EN EL SISTEMA CL@VE

El Reglamento eIDAS emplaza a la Comisión Europea a establecer (a más tardar el 18 de septiembre de 2015) mediante actos de ejecución, las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica.

Estas especificaciones técnicas mínimas, normas y procedimientos se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:

1. el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica;
2. el procedimiento para expedir los medios de identificación electrónica solicitados;
3. el mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria;
4. la entidad que expide los medios de identificación electrónica;
5. cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica;
6. las especificaciones técnicas y de seguridad de los medios de identificación electrónica.

Por otra parte, el reglamento eIDAS tendrá en cuenta los resultados de STORK y la norma ISO 29115 a la hora de determinar los niveles de seguridad. En particular, en el considerando 16 se establece que: "[…]*Como resultado de las actividades la normalización y las actividades internacionales de la financiación de la Unión de proyectos piloto a gran escala, existen varias definiciones y descripciones técnicas de niveles de seguridad. En particular, los proyectos piloto a gran escala STORK e ISO 29115 se refieren, entre otros, a los niveles 2, 3 y 4 que deben tenerse en cuenta en la máxima medida para establecer los requisitos técnicos mínimos, las normas y los procedimientos para los niveles de seguridad bajo, sustancial y alto entendidos en el sentido del presente Reglamento, garantizando al mismo tiempo la aplicación coherente del presente Reglamento, en particular con respecto al nivel de seguridad alto en relación con la acreditación de identidad para la expedición de certificados cualificados.*[…]".

Es por ello que, aunque no estén definidas todavía las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad del Reglamento, se puede asumir razonablemente la siguiente correspondencia entre los niveles de QAA de STORK, los niveles definidos en la norma ISO 29115, y los niveles de seguridad del reglamento eIDAS:

Nivel QAA STORK	Nivel ISO 29115	Nivel de seguridad eIDAS
1	1 – Bajo	No previsto
2	2 - Medio	Bajo
3	3 – Alto	Sustancial
4	4 – Muy alto	Alto

Teniendo en cuenta lo anterior, y los requisitos establecidos tanto en el modelo QAA de STORK como en la norma ISO 29115 para cada uno de los niveles, en el sistema Cl@ve se han identificado los siguientes niveles de seguridad, asociados a las distintas modalidades de identificación permitidas en el sistema:

Nivel en Cl@ve	Nivel de Registro	Modo de registro	Credencial	Nivel ENS
2 (bajo)	Básico	Telemático a partir de datos conocidos, basado en CSV	Clave PIN Clave Permanente sin OTP	BAJO
	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave Permanente sin OTP	
3 (medio)	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave PIN Clave Permanente reforzada con OTP (SMS al móvil) Certificado reconocido en soporte SW	MEDIO
4 (alto)	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	DNI electrónico Otros certificados reconocidos en soporte HW, con la certificación de una entidad de certificación acreditada.	ALTO

La idoneidad de los sistemas equivalentes a que se hace referencia en la columna de Modo de registro, deberá ser confirmada por un organismo de evaluación de la conformidad, según el artículo 24.1.d) del Reglamento eIDAS.

Se entiende que el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica es fuerte cuando el registro se haga presencialmente o mediante un certificado electrónico reconocido. Y que es básico cuando se base en la aportación de datos conocidos por ambas partes.

De igual modo, se asume que la identificación tendrá un nivel de seguridad medio cuando se base al menos en dos factores: algo que se sabe y algo que se tiene.

Queda así restringido el nivel alto al proporcionado por el DNI electrónico u otro certificado electrónico reconocido en tarjeta criptográfica, que disponga de la certificación correspondiente de una entidad de certificación acreditada.

Se ha optado por usar como criterio principal para la asignación de niveles de seguridad en la identificación el ENS, estableciendo una equivalencia entre las dos clasificaciones, la del ENS y la de Cl@ve, de tal manera que se seleccione el nivel de seguridad en la identificación de Cl@ve (bajo, medio o alto) en función del nivel de seguridad requerido, respecto de la autenticidad, por nuestro sistema de información (bajo, medio o alto), tras la categorización del mismo y según los criterios marcados por el ENS.

Este criterio se podrá adaptar en aplicación del principio de proporcionalidad, siempre y cuando se justifique que se protege igual o mejor el riesgo sobre los activos mediante la implantación de medidas compensatorias de otra índole.

Si el procedimiento o servicio que pretendemos integrar con Cl@ve está ya adaptado al ENS, se habrá categorizado (informalmente o a través de un proceso riguroso de análisis de riesgos) y tendrá asignado un nivel de seguridad, que determinará unívocamente el nivel de identificación de Cl@ve.

Si no es así, el proceso a seguir deberá ser el siguiente:

Para cada servicio/procedimiento cuyo acceso se debe regular con la plataforma Cl@ve se deberán identificar aquellos activos de información que puedan verse comprometidos por algún incidente de seguridad que afecte a las dimensiones de autenticidad y confidencialidad, únicas de aplicación en este caso.

Para cada activo de información se evaluará el impacto que para la organización tendría que se accediese en consulta o modificación de datos por una persona no autorizada. Para ello se emplearán los criterios del ENS mencionados en el punto anterior.

El mayor nivel de seguridad requerido entre todos los activos de información determinará el nivel de identificación de Cl@ve.