

**Especificación de Requisitos**

*Cl@ve2 - Monitorización*

**Solución de Monitorización (Cl@ve 2)**

Versión 29/10/2018

Control de Modificaciones

|  |  |
| --- | --- |
| Documento nº: | Cl@ve-Monitorizacion-REQ |
| Revisión: | 001 |
| Fecha: | 29/10/2018 |

|  |  |
| --- | --- |
| Rev. | 001 |
| Fecha | 29/10/2018 |
| Descripción | Versión inicial del documento |

Control de Distribución

|  |  |
| --- | --- |
| Documento nº: | Cl@ve-Monitorizacion-REQ |
| Revisión: | 001 |
| Fecha: | 29/10/2018 |

Propiedad del documento:

Este documento pertenece al Gobierno de España y posee un carácter de público para uso y distribución en ámbitos autorizados por este mismo, según se recoge en la declaración de privacidad.

Declaración de privacidad:

El contenido de este documento está sujeto al protocolo de libre distribución dentro del entorno definido para el contexto.

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

**INDICE GENERAL**

[1 Objeto 5](#_Toc531630131)

[2 Alcance 5](#_Toc531630132)

[3 Siglas 6](#_Toc531630133)

[4 Documentos de Referencia 6](#_Toc531630134)

[5 Descripción de la Situación Actual 7](#_Toc531630135)

[6 Definición de Requisitos 8](#_Toc531630136)

[6.1 Requisitos Funcionales 8](#_Toc531630137)

[6.1.1.1 REQ-FNC-001 / Monitorización real del servicio 8](#_Toc531630138)

[6.1.1.2 REQ-FNC-002 / Solicitud monitorización 9](#_Toc531630139)

[6.1.1.3 REQ-FNC-003 / Monitorización del componente pasarela 9](#_Toc531630140)

[6.1.1.4 REQ-FNC-004 / Monitorización del componente IdP @firma 10](#_Toc531630141)

[6.1.1.5 REQ-FNC-005 / Publicación y consulta del estado del servicio 11](#_Toc531630142)

[6.1.1.6 REQ-FNC-006 / Configuración y administración del sistema 11](#_Toc531630143)

[6.1.1.7 REQ-FNC-007 / Comunicación de alarma 12](#_Toc531630144)

[6.1.1.8 REQ-FNC-008 / Explotación de información de estado 12](#_Toc531630145)

[6.2 Requisitos no Funcionales 12](#_Toc531630146)

[6.2.1 Requisitos de Información 12](#_Toc531630147)

[6.2.1.1 REQ-FNC-008 / Usuario 12](#_Toc531630148)

[6.2.1.2 REQ-INF-002 / Plataforma 13](#_Toc531630149)

[6.2.1.3 REQ-INF-003 / Funcionalidad testeada 13](#_Toc531630150)

[6.2.1.4 REQ- INF-004 / Temporizador 13](#_Toc531630151)

[6.2.2 Requisitos de Seguridad 14](#_Toc531630152)

[6.2.2.1 REQ- SEG-001 / Control de acceso 14](#_Toc531630153)

[6.2.3 Requisitos Técnicos 14](#_Toc531630154)

[6.2.3.1 REQ- TEC-001 / Monitoriz@ 14](#_Toc531630155)

[6.2.4 Requisitos de Integración 15](#_Toc531630156)

[6.2.4.1 REQ- INT-001 / Comunicación con sistemas de información monitorizados 15](#_Toc531630157)

# Objeto

Este documento tiene por objeto recopilar y ofrecer una descripción completa de las necesidades y objetivos, tanto funcionales, como no funcionales, que deben ser satisfechos por el nuevo Sistema de monitorización de Cl@ve.

# Alcance

El objetivo del documento es ofrecer una Especificación de Requisitos del nuevo Sistema de monitorización de Cl@ve, basándose para ello en las características y necesidades expresadas en el requisito funcional FUN-12 del pliego de preinscripciones técnicas del expediente 3335.

Para ello, este documento presentará la siguiente información:

1. Situación actual del sistema.
2. Requisitos, necesidades y restricciones del sistema, organizándolas en las siguientes categorías:
   1. Requisitos funcionales. Estos requisitos determinan el comportamiento del sistema, y establecen el conjunto de funcionalidades dispuestas y ofrecidas por el mismo.
   2. Requisitos no funcionales. características del sistema que aplican de forma general a toda la organización.
      1. Requisitos de información. Estos requisitos deben especificar qué información debe almacenar el sistema para poder ofrecer las funcionalidades demandadas.
      2. Requisitos tecnológicos, los cuales a su vez se dividen en las siguientes categorías:
         1. Arquitectura.
         2. Integración, interacción y comunicación con otros sistemas de información.
      3. Otros requisitos no funcionales.

# Siglas

|  |  |
| --- | --- |
| **HTTP** | *Hypertext Transfer Protocol* |
| **HTTPS** | *Hypertext Transfer Protocol Secure* |
| **IdP** | *Identity Provider – Proveedor de Identidad* |
| **MINPTFP** | *Ministerio de Política Territorial y Función Pública* |
| **SAML** | *Security Assertion Markup Language* |
| **SOAP** | *Simple Object Access Protocol* |
| **SP** | *Service Provider* – Proveedor de Servicios |
| **URL** | Uniform Resource Locator |
| **WAR** | *Web Application Archive* - Archivo de aplicación web |

# Documentos de Referencia

|  |  |
| --- | --- |
| **Manual de Monitoriz@** |  |
| **Analisis\_Requisitos\_sol monitorizacion** |  |
| **Acta de reunión de trabajo 18/10/2018** | 24981 - MAP - ACT 20181018 V.1.2 |

# Descripción de la Situación Actual

El sistema de identificación Cl@ve actualmente no incluye o integra ningún sistema o módulo que permita conocer el estado de disponibilidad de las diferentes funcionalidades que pone a disposición de sus usuarios finales, tanto a los responsables del sistema, como a los responsables de los sistemas integrados con Cl@ve. Esta situación dificulta la mantenibilidad del sistema, impidiendo llevar a cabo actuaciones preventivas que puedan evitar una degradación o, incluso, una caída parcial o total del sistema.

Cl@ve, además, presenta ciertos aspectos que hacen más compleja la labor de monitorización completa de los diferentes mecanismos de identificación que ofrece (extremo a extremo). Estos son los siguientes:

* **Arquitectura distribuida**. Los principales componentes pertenecientes al sistema que participan en procesos de identificación son los siguientes:
  + **Pasarela**. Componente principal del Sistema que actúa como proxy o fachada, siendo el componente responsable de recibir las peticiones de identificación efectuadas por los SP’s y redirigirlas a los IDP’s destino del proceso de identificación.
  + **IdP - @firma**. Componente que implementa el IdP responsable de llevar a cabo la autenticación de un usuario mediante un certificado electrónico, integrándose para ello con la plataforma @firma, sistema que permitirá conocer su estado de validación y obtener la información incluida en el certificado.
* **Número de integraciones con otros sistemas elevado**. Cl@ve actúa como intermediario entre el SP que inicia el proceso de identificación, y el IdP destino del proceso (PIN 24h, PIN permanente, IdP - @firma y el nodo eIDAS español), habilitando la selección o establecimiento del mecanismo autenticación, tanto a usuarios, como a los propios SP’s. Esto implica que el Sistema debe poder interactuar con los sistemas de información responsables de informar la identidad del usuario, IdP’s, influyendo estos, por tanto, en la correcta resolución de los procesos de identificación.
* **Modelo de comunicación entre componentes**. El modelo de comunicación en SP’s, Cl@ve y los eIDAS está basado en el intercambio de mensajes SAML, enviados de un sistema a otro mediante redirecciones efectuadas a través del navegador del usuario objeto del proceso de identificación. Este modo de funcionamiento complica la verificación completa del estado del Sistema, mediante medios automáticos, aunque si permite la realización de pruebas sobre los principales componentes del Sistema, de forma que, en función de los indicadores obtenidos sobre estos, se puede determinar el estado del Sistema completo-

No obstante, y como parte de los trabajos a realizar en el expediente 3114, relativo al mantenimiento y evolución de la suite de @firma, se está desarrollando el sistema de información Monitoriz@. Este sistema de información proporciona mecanismos que habilitan el seguimiento del estado de sistemas que publican sus servicios mediante web services SOAP y otros protocolos, permitiendo la definición de umbrales de calidad del servicio, la recolección de métricas sobre los sistemas monitorizados, la gestión del envío de alarmas por cambios de estado o mal funcionamiento, o la frecuencia de testeo de cada sistema.

Estas funcionalidades, así como otras funcionalidades solicitadas para este nuevo componente de la plataforma Cl@ve, son satisfechas por Monitoriz@, convirtiéndose, de este modo, en el sistema de información sobre el que se implementará el módulo de monitorización.

# Definición de Requisitos

Este apartado recopila los requisitos que deben ser satisfechos por el sistema de monitorización de la plataforma Cl@ve.

La nomenclatura empleada para codificar los requisitos será **REQ-YYY-NNN**, donde:

* YYY hace referencia al tipo de requisito:
  + Requisito Funcional: FNC.
  + Requisito No Funcional.
    - Requisitos de información: INF.
    - Requisitos de seguridad: SEG.
    - Requisitos tecnológicos: TEC.
    - Requisitos de Integración: INT.
* CAINNNN es el número del requisito.

## Requisitos Funcionales

Los requisitos funcionales que debe satisfacer el nuevo módulo de monitorización de la plataforma Cl@ve son definidos y descritos en los siguientes apartados.

#### REQ-FNC-001 / Monitorización real del servicio

| REQ-FNC-001 | Monitorización real del servicio | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe permitir llevar a cabo el seguimiento sobre el funcionamiento real del servicio, extremo a extremo, de forma que se compruebe completamente el estado de los diversos componentes del Sistema que intervienen en los procesos de identificación.  El sistema de monitorización admitirá la verificación de cada nodo del Sistema individualmente, así como de la VIP, facilitando la configuración del conjunto de peticiones de prueba que serán lanzadas para determinar el estado del Sistema. | | |
| Datos específicos | Peticiones lanzadas para verificar el estado del Sistema. Las peticiones de cada servicio o Sistema pueden tener diferente formato, e incluir información diferente, pudiendo, además, ser generadas en tiempo real. | | |
| Comentarios | Queda fuera del alcance la monitorización de los IdP PIN 24H y Cl@ve permanente | | |

#### REQ-FNC-002 / Solicitud monitorización

| REQ-FNC-002 | Solicitud monitorización | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe implementar los mecanismos necesarios para lanzar peticiones de identificación de prueba de forma periódica y automática, o de modo manual, por petición expresa de un usuario administrador del Sistema. | | |
| Datos específicos | N/A | | |
| Comentarios | N/A | | |

#### REQ-FNC-003 / Monitorización del componente pasarela

| REQ-FNC-003 | Monitorización de Pasarela | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe ser capaz de verificar el estado de disponibilidad del componente pasarela mediante el envío de una petición SAML mediante HTTP, generada en tiempo real, que este componente emplea posteriormente para redirigir al usuario al IdP destino del proceso de identificación. | | |
| Datos específicos | El agente de monitorización que implemente este mecanismo debe permitir configurar los siguientes parámetros:   * Petición HTTP.   + Establecimiento de conexión.     - Servidor proxy.   + Cabeceras HTTP.   + Parámetros HTTP. * Petición SAML.   + Parámetro assertionConsumerServiceURL.   + Elemento SPApplication.   + Parámetro providerName.   + Elemento SPType.   + Atributos de identificación solicitados (admitidos por eIDAS para persona física). | | |
| Comentarios | N/A | | |

#### REQ-FNC-004 / Monitorización del componente IdP @firma

| REQ-FNC-004 | Monitorización de IdP @firma | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe ser capaz de verificar el estado de disponibilidad del componente IdP @firma de la plataforma, debiendo enviar mediante HTTP, que aporte el certificado electrónico mediante el que será autenticado el usuario, y una petición SAML, generada en tiempo real. | | |
| Datos específicos | El agente de monitorización que implemente este mecanismo debe permitir configurar los siguientes parámetros:   * Petición HTTP.   + Establecimiento de conexión.     - Servidor proxy.     - Certificado electrónico empleado en la securización del canal de comunicación por el usuario.   + Cabeceras HTTP.   + Parámetros HTTP. * Petición SAML.   + Parámetros assertionConsumerServiceURL.   + Elemento SPApplication.   + Parámetro providerName.   + Elemento SPType.   + Atributos de identificación solicitados (admitidos por eIDAS para persona física). | | |
| Comentarios | N/A | | |

#### REQ-FNC-005 / Publicación y consulta del estado del servicio

| REQ-FNC-005 | Publicación y comunicación de estado del servicio | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe permitir a los responsables del sistema (prioritario), y de los organismos cuyos sistemas se integran con Cl@ve, conozcan en todo momento del estado de los diferentes nodos y componentes que conforman el Sistema.  La información de monitorización se publicará como un servicio en la Red Sara (Servicio web y web) de manera que las aplicaciones y organismos usuarios puedan determinar el grado de disponibilidad de la plataforma. | | |
| Datos específicos | Información de disponibilidad de cada uno de los componente y nodos monitorizados (estado, tiempo medio respuesta, etc.). | | |
| Comentarios | N/A | | |

#### REQ-FNC-006 / Configuración y administración del sistema

| REQ-FNC-006 | Configuración y administración del sistema | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe admitir la configuración y gestión de aspectos comunes, requeridos para el correcto funcionamiento del sistema, así como todos aquellos datos y parámetros requeridos para llevar a cabo el seguimiento sobre el funcionamiento de los sistemas monitoreados. | | |
| Datos específicos | Información y parámetros que deben poder ser configurados por sistema de monitorización son los siguientes:   * Servidor proxy. * Comunicación con servidor de correo electrónico. * Certificados de confianza utilizados en comunicaciones seguras. * Plataformas o sistemas de información monitorizados, y mecanismo empleado para su monitorización. * Parámetros para la monitorización, como por ejemplo, agente de control responsable de lanzar las pruebas, intervalos, retardos o umbrales de degradación de servicio a partir de los cuales se lanzarán alarmas. | | |
| Comentarios | N/A | | |

#### REQ-FNC-007 / Comunicación de alarma

| REQ-FNC-007 | Comunicación de alarmas | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe permitir la comunicación de alertas a los responsables del Sistema, y de los responsables de los organismos, mediante correo electrónico, SMS y agente (Graylog), en el caso de que se detecte algún comportamiento anómalo, o degradación (a partir de la definición de umbrales), de los servicios y sistemas monitorizados. | | |
| Datos específicos | * Umbrales por servicio o sistema de monitorización monitorizado. * Datos de contacto de responsables. | | |
| Comentarios | N/A | | |

#### REQ-FNC-008 / Explotación de información de estado

| REQ-FNC-008 | Comunicación de alarmas | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe generar informes configurables sobre faltas de disponibilidad, degradación del uso, tiempos de respuesta, etc. | | |
| Datos específicos | N/A | | |
| Comentarios | N/A | | |

## Requisitos no Funcionales

### Requisitos de Información

#### REQ-FNC-008 / Usuario

| REQ-INF-001 | Usuario | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe almacenar y gestionar información sobre los responsables del Sistema, y responsables de los organismos integrados con la plataforma Cl@ve | | |
| Datos específicos | * Datos de identificación. * Datos de control de acceso. * Datos de contacto y comunicación. | | |
| Comentarios | N/A | | |

#### REQ-INF-002 / Plataforma

| REQ-INF-002 | Plataforma | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe gestionar información sobre los servicios y sistemas de información monitorizados. | | |
| Datos específicos | * Denominación. * Acceso al servicio o sistema de información monitorizado. | | |
| Comentarios | N/A | | |

#### REQ-INF-003 / Funcionalidad testeada

| REQ-INF-003 | Funcionalidad testeada | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe gestionar información sobre las diferentes funcionalidades de los servicios o sistemas de información que serán objeto de seguimiento y testeo. | | |
| Datos específicos | * Mecanismo de testeo. * Información complementaria sobre el acceso a la funcionalidad testeada. * Batería de peticiones de pruebas. * Umbrales de degradación. | | |
| Comentarios | N/A | | |

#### REQ- INF-004 / Temporizador

| REQ-INF-004 | Temporizador | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe administrar las entidades responsables de lanzar automáticamente y periódicamente las pruebas que permitirán conocer el estado de disponibilidad de las diferentes funcionalidades testeadas. | | |
| Datos específicos | * Frecuencia de lanzamiento. * Relación de funcionalidades testeadas. | | |
| Comentarios | N/A | | |

### Requisitos de Seguridad

#### REQ- SEG-001 / Control de acceso

| REQ-SEG-001 | Control de acceso | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe admitir identificar a los usuarios que interactúen con él, a través de su interfaz gráfico, mediante credenciales usuario/password, o certificado electrónico. | | |
| Datos específicos | N/A | | |
| Comentarios | N/A | | |

### Requisitos Técnicos

#### REQ- TEC-001 / Monitoriz@

| REQ-TEC-001 | Control de acceso | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de información Monitoriz@ se constituye como el sistema base para la gestión de los agentes de monitorización, alarmas y resto de funcionalidades esperadas para este sistema, y expresadas en el pliego de preinscripciones. | | |
| Datos específicos | N/A | | |
| Comentarios | El equipo de proyecto de Cl@ve es responsable del desarrollo y mantenimiento de los componentes de Cl@ve que se integren en Monitoriz@, pero no de la evolución y mantenimiento de la propia aplicación Monitoriz@.  Este sistema ya implementa mecanismos de monitorización que permiten lanzar pruebas de testeo sobre los siguientes servicios o sistemas de información:   * Servicios web SOAP. * TS@. * Servicio OCSP. | | |

### Requisitos de Integración

#### REQ- INT-001 / Comunicación con sistemas de información monitorizados

| REQ-INT-001 | Comunicación con sistemas de información monitorizados | | |
| --- | --- | --- | --- |
| Versión | 01.00 | **Estado** | Propuesto |
| Dependencias | N/A | | |
| Descripción | El sistema de monitorización debe poder comunicarse e invocar las funcionalidades testeadas de los servicios o sistemas de información monitorizados. | | |
| Datos específicos | N/A | | |
| Comentarios | N/A | | |