Resumen de los protocolos de seguridad del Registro Telemático

1 Introducción

La gestión de seguridad del Registro Telemático tiene los siguientes fines [1]:

- Identificar, autenticar y, en su caso, autorizar el acceso a los sistemas de información
- Identificar fidedignamente a remitente y destinatario de las comunicaciones electrónicas
- Controlar el acceso para restringir la utilización y el acceso a datos e informaciones a las personas autorizadas y proteger los procesos informáticos frente a manipulaciones no autorizadas
- Mantener la integridad de la información y elementos del sistema, para prevenir alteraciones o pérdidas de los datos e informaciones
- Garantizar la disponibilidad de la información y de las aplicaciones
- Prevenir la interceptación, alteración y acceso no autorizado a la información
- Gestionar las incidencias de seguridad
- Auditar y controlar la seguridad

La aplicación del Registro Telemático cumple con los fines descritos mediante la utilización de estándares reconocidos y tecnologías probadas, y desarrollada siguiendo las metodologías actuales. Este documento detalla los criterios de seguridad aplicados al diseño, desarrollo e implantación de la aplicación en el Ministerio de Sanidad y Consumo.

2 Criterios de Seguridad

2.1 Gestión global de la seguridad

Este documento se refiere exclusivamente a la seguridad del Registro Telemático y de los datos manejados por el mismo.

2.2 Política de seguridad

La seguridad del sistema debe garantizar:

- Autenticidad
- Confidencialidad
- Integridad
- Disponibilidad

2.2.1 Autenticidad

Autenticidad es la identificación de los actores implicados en el registro de datos en el Registro Telemático. Ésta se garantiza mediante la firma digital, conexiones SSL con autenticación de cliente y validación de certificados.
Los capítulos Transporte y Autenticación detallan los procesos necesarios para garantizar la autenticidad.

2.2.2 Confidencialidad

La *confidencialidad* se refiere a controlar el acceso a los datos a las partes implicadas en el registro de datos en el Registro Telemático, tanto durante el registro (protección de transporte) como al posterior almacenamiento de los datos.
El capítulo Confidencialidad detalla los procesos necesarios para garantizar la confidencialidad.

2.2.3 Integridad

La integridad de las peticiones a la aplicación del Registro Telemático contempla el "no repudio", la trazabilidad y el evitar la modificación no detectada y/o controlada de los datos una vez registrados. El uso de la firma electrónica garantiza la integridad de los datos que entran en el Registro Telemático, mientras el diseño de la aplicación garantiza la detección de modificaciones posteriores a los datos, aunque no puede evitarla.
Los capítulos Integridad y Firma electrónica detallan los procesos aplicados para garantizar la integridad.

2.2.4 Disponibilidad

El servicio debe estar disponible de forma permanente (24-7); actualizaciones y arreglos del servicio no deben suponer una limitación. El servicio debe ser resistente a ataques tipo "denegación de servicio", intrusión y código dañino ("inyectado").

2.3 Organización y planificación de la seguridad

El Ministerio de Sanidad y Consumo ha realizado la organización y planificación de la seguridad siguiendo los criterios establecidos en el documento "Criterios de seguridad, normalización y conservación", del Ministerio de Administraciones Públicas.

2.4 Análisis y gestión de riesgos

El Ministerio de Sanidad y Consumo ha realizado un Análisis de Gestión de Riesgos de sus sistemas de información [2], de acuerdo a MAGERIT 2 y soportado con la herramienta PILAR.

2.5 Identificación y clasificación de activos a proteger

Los datos recibidos por el Registro Telemático son de cuatro tipos:

- Datos comunes de todos los formularios (datos necesarios para cumplir con SICRES 2.0 [3])
- Datos completos de los formularios
- Ficheros adjuntos
- Números de registro (general y oficina) y fecha de los mismos

2.5.1 Datos comunes

Estos datos se guardan en la base de datos, cuyo acceso está permitido desde la aplicación de Registro.

2.5.2 Datos completos de los formularios

Los datos completos de los formularios incluyen información clasificada de nivel Básico según el RD 994/1999 art. 3, cumpliendo las medidas de seguridad exigidos para dicho nivel.
Esta información incluye los datos de contacto del peticionario, y texto de carácter libre cuyo contenido no está definido.
Se guarda en:

- Log de trazas (accesible para el personal con permisos en el servidor)
- Sistemas de gestión del Ministerio de Sanidad y Consumo (accesibles para el personal con permisos en las aplicaciones)

2.5.3 Ficheros adjuntos

Un usuario puede adjuntar ficheros con datos adicionales para su petición; el contenido de los ficheros no está definido. Los ficheros se guardan en disco. El Ministerio de Sanidad y Consumo realiza una auditoria del acceso a dichos ficheros.

2.5.4 Números de registro

Los números de registro asignados a una petición se guardan en la base de datos, y se pasan a la aplicación de Calidad. Son accesibles por lo tanto desde tres sitios:

- Registro Telemático, servicio web de consulta (aplicación no disponible desde fuera del Ministerio, y con control de acceso desde dentro)
- Aplicación de Registro
- Aplicaciones de gestión del Ministerio de Sanidad y Consumo.

2.6 Salvaguardas ligadas al personal

La definición de funciones y obligaciones del personal, la educación del personal de sus responsabilidades, la asignación de puestos, etc., está definida en el documento Política de Seguridad del Ministerio de Sanidad y Consumo.

2.7 Seguridad física

La seguridad física de los sistemas implicados en el Registro Telemático está definida en el documento Política de Seguridad del Ministerio de Sanidad y Consumo.

2.8 Autenticación

La autenticación está garantizada por dos mecanismos:

- El proceso de firma digital, con su correspondiente proceso de verificación de firma y de la validez del certificado usado para la firma.
- La conexión a los formularios está basado en SSL con autenticación de cliente, obligando así al usuario autenticarse con su certificado digital.

Actualmente se soporta certificados emitidos por los siguientes emisores:

- ANF (ANF Autoridad de Certificación)
- CAGVA (Autoridad de Certificación de la Generalidad Valenciana)
- CAMERFIRMA (Autoridad de certificación digital de las Cámaras de Comercio españolas)
- CATCERT (Agencia Catalana de Certificación (ACC))
- FNMT (Fábrica Nacional de Moneda y Timbre)
- IZENPE (Autoridad de Certificación Vasca)
- e-DNI (Documento Nacional de Identidad electrónico)
- FIRMAPROFESIONAL (Entidad de certificación digital dirigida a corporaciones profesionales y otras instituciones)
- BANESTO (Banco Español de Crédito, S.A)

El Ministerio proporciona el servicio de validación de los certificados.

2.9 Confidencialidad

Existen dos riesgos para la confidencialidad de los datos personales manejados por el Registro Telemático:

- Transporte
- Almacenamiento

2.9.1 Transporte

La confidencialidad está garantizada mediante el uso exclusivo de conexiones tipo SSL.

2.9.2 Almacenamiento

El apartado “Identificación y clasificación de activos a proteger” trata con más detalle los datos guardados y su almacenamiento.

2.10 Integridad

La integridad de los datos recibidos por el Registro Telemático está garantizada por el uso de firma digital, lo que permite la verificación de la integridad de los datos en el momento del registro. La firma permanece guardada en la base de datos, permitiendo también una verificación posterior de los datos, tanto los de los formularios como de cualquier fichero que se ha adjuntado.

2.11 Disponibilidad

El Ministerio de Sanidad y Consumo dispone de infraestructuras de respaldo para garantizar la máxima disponibilidad de la aplicación (comunicaciones, servidores, almacenamiento y copias de respaldo).

2.12 Control de acceso

Por su propia naturaleza la aplicación del Registro Telemático está abierta a acceso por ciudadanos; no hay usuarios dados de alta en el sistema. El derecho a acceso es libre a toda persona con certificado digital válido, y no está contemplado limitar el acceso a usuarios determinados. La identificación del ciudadano está detallada en el apartado “Autenticación”.

El control de acceso a la base de datos y los servidores está definido en el documento Política de Seguridad del Ministerio de Sanidad y Consumo.

2.13 Acceso a través de redes

La seguridad del acceso a través de redes está definida en el documento Política de Seguridad del Ministerio de Sanidad y Consumo.

2.14 Firma electrónica

Todas la peticiones al Registro Telemático están firmadas en el cliente y validados en el servidor antes de registrarse.

2.14.1 Firma en el cliente

Cuando un cliente descarga el formulario a su navegador este formulario incluye embebido un componente de firma (ActiveX si utiliza Internet Explorer, o Applets si utiliza Netscape, Firefox o Mozilla). El formulario usa javascript para pasar la información a firmar al componente, y este segundo accede al almacén de certificados del navegador para firmar los datos y ficheros adjuntos (si los hay). La información del formulario y la(s) firma(s) asociada(s) se mandan al servidor.

2.14.2 Validación en el servidor

La validación de las firmas en el servidor sigue el siguiente protocolo:

- Validación de la firma con los datos
- Validación de que el certificado asociado ha sido emitido por una autoridad de confianza, y de que no ha sido revocado.

Si falla cualquiera de los dos, la petición se rechaza.

2.15 Protección de soportes y copias de respaldo

La seguridad de la protección de soportes y copias de respaldo está definida en el documento Política de Seguridad del Ministerio de Sanidad y Consumo.

2.16 Desarrollo y explotación de sistemas

Las actualizaciones de la aplicación del Registro Telemático siguen los pasos recomendados por el Ministerio de Sanidad y Consumo:

- Desarrollo – modificaciones nuevas, pruebas en el entorno del Ministerio
- Preproducción – versiones de release, en un entorno estable. Pruebas de terceros.
- Producción – versión de release.

2.17 Auditoria y control de la seguridad

El Ministerio de Sanidad y Consumo realiza una auditoria del control de la seguridad cada 2 años.

3 Referencias

[1] Criterios de seguridad, normalización y conservación, Ministerio de Administraciones Públicas (24 de junio de 2004), pp 1-2
[2] Informe Hacking Ético-2006-01-00 Burke
[3] Datos de intercambio SICRES 2.0, Ministerio de Fomento (22 de septiembre de 1999)