

CÁMARA DE CUENTAS DE ANDALUCÍA

RESUMEN DE INFORME

AUDITORÍA DE CUMPLIMIENTO DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS DEL SISTEMA DE RECETA MEDICA ELECTRÓNICA DEL SERVICIO ANDALUZ DE SALUD (SAS)

Ejercicio 2021

El Pleno de la Cámara de Cuentas de Andalucía incluyó en el Plan de Actuaciones para el ejercicio 2021 una “Auditoría de cumplimiento de ciberseguridad y protección de datos del sistema de receta médica electrónica del Servicio Andaluz de Salud (SAS)”.

Se trata de una fiscalización sobre controles de ciberseguridad, y abre una nueva línea de actuación por la Cámara de Cuentas de Andalucía (CCA), encaminada a la verificación del cumplimiento del Esquema Nacional de Seguridad (ENS) y de protección de datos.

El ENS se aplica a todo el sector público y a los sistemas que tratan información clasificada, así como a los sistemas de información de las entidades del sector privado, cuando presten servicios o provean soluciones a las entidades del sector público, para el ejercicio de sus competencias y potestades administrativas.

Ante estas medidas de seguridad, condicionadas al nivel de seguridad (autenticidad, integridad, confidencialidad, trazabilidad, disponibilidad) y a la categoría del sistema de información de que se trate (básica, media, alta), se establece la necesidad de verificar y de controlar el cumplimiento de los requerimientos del ENS y de protección de datos. Al SAS le resulta de aplicación y de obligado cumplimiento el ENS.

En el año 2003 se inició por el SAS, en colaboración con Consejo Andaluz de Colegios Oficiales de Farmacéuticos (en adelante CACOF), el proyecto de receta electrónica que se denomina Receta XXI. La receta médica y las órdenes de dispensación, como documentos normalizados, suponen un medio fundamental para la transmisión de información entre los profesionales sanitarios y una garantía para el paciente.

La Cámara de Cuentas de Andalucía asume en este informe un compromiso de atestiguamiento, consistente en expresar una opinión en términos de seguridad razonable, basada en la fiscalización realizada, del modelo de gobierno y gestión de la seguridad implantado por el SAS en el contexto del entorno de Receta XXI. De esta manera, se valora si el funcionamiento desde la prescripción hasta la dispensación del medicamento respeta las medidas recogidas en el anexo II del ENS y la normativa de protección de datos.

La auditoría se ha realizado de conformidad con los Principios fundamentales de fiscalización de las Instituciones Públicas de Control Externo (ICEX). Concretamente, las ISSAI-ES 100 “Principios fundamentales de fiscalización del sector público,” ISSAI-ES 400 “Principios fundamentales de la fiscalización de cumplimiento,” y las guías prácticas de fiscalización GPF-OCEX 4000 “Guía para las auditorías de cumplimiento” y GPF-OCEX 4320 “Guía sobre la importancia relativa en las fiscalizaciones de cumplimiento de la legalidad”, así como la serie de GPF 5300, más concretamente la GPF_OCEX 5311 “Ciberseguridad, seguridad de la información y auditoría externa”, GPF-OCEX 5312 “Glosario de Ciberseguridad” y GPF-OCEX 5313 “Revisión de los controles básicos de ciberseguridad”.

CÁMARA DE CUENTAS DE ANDALUCÍA

RESUMEN DE INFORME

Estas normas exigen que la Cámara de CCA cumpla los requerimientos de ética, y que planifique y ejecute la auditoría con el fin de obtener una seguridad razonable de que el funcionamiento del proceso Receta XXI se adecue, en todos los aspectos significativos, con la normativa de aplicación.

El ámbito subjetivo de la fiscalización comprende las actuaciones en materia de seguridad y protección de datos llevadas a cabo por el SAS, por lo que la fiscalización se desarrolla con las garantías metodológicas y de independencia, profesionalidad y adecuación requerida. El alcance temporal de la fiscalización ha sido el año 2021.

En el informe también se ha tenido en cuenta el cumplimiento de la legislación vigente de seguridad y de protección de datos en las farmacias, ya que éstas son el enlace directo entre el usuario final y el SAS. Este entorno de información actúa como soporte al servicio de receta electrónica del SAS, en el contexto de la gestión de la atención sanitaria. Por ello, los trabajos de fiscalización se han ampliado para incorporar una muestra de tres oficinas de farmacia identificadas por el CACOF, en la medida que estas son el enlace directo entre el paciente y el SAS. Así, la auditoría que afecta únicamente al SAS, ha permitido revisar las actuaciones de las oficinas de farmacia seleccionadas como usuarios del entorno de información de Receta XXI.

Sobre el cumplimiento del Esquema Nacional de Seguridad

Opinión con salvedades

En opinión de la Cámara de Cuentas de Andalucía, excepto por los incumplimientos descritos en el apartado del informe de “Fundamentos de la opinión con salvedades del ENS”, el modelo de gobierno y gestión de la seguridad implantado por el SAS, en el contexto del entorno de Receta XXI, cumple en todos los aspectos significativos con la normativa de aplicación.

Los principales incumplimientos incluidos en el informe son:

Se incumple la medida que exige la singularidad de la identificación como elemento base del acceso al sistema. Todo usuario ha de emplear un identificador único determinado por su rol, de tal manera que garantice saber quién y qué derechos de acceso recibe, y qué ha realizado. Además, se ha detectado el uso compartido de cuentas de usuario.

En los mecanismos de autenticación frente al sistema, se pueden usar diferentes factores de autenticación¹. Se ha comprobado que no se ha implementado el doble factor de autenticación.

Se deben recopilar los datos necesarios para conocer el grado de implantación de las medidas de seguridad, para llevar a cabo el informe anual requerido ENS. El SAS no tiene implementada dicha medida.

¹ El doble factor de autenticación consiste en emplear dos métodos de naturaleza distinta para poder acceder al sistema o a la aplicación. Dentro de estas naturalezas se encuentra, algo que el usuario sabe (ej. Clave), algo que el usuario tiene (ej. Tarjeta criptográfica) y algo que el usuario es (ej. Iris del ojo).

CÁMARA DE CUENTAS DE ANDALUCÍA

RESUMEN DE INFORME

Los equipos informáticos deberían bloquear sus pantallas transcurrido un cierto tiempo de inactividad, impidiendo su utilización por personas no autorizadas. Esta medida no está implantada en la actualidad.

Sobre el cumplimiento de protección de datos

Opinión con salvedades

En opinión de la Cámara de Cuentas de Andalucía, excepto por los incumplimientos descritos en el apartado el informe “Fundamentos de la opinión con salvedades de Protección de Datos”, el modelo de gobierno y gestión de la privacidad implantado por el SAS, en el contexto del entorno de Receta XXI, cumple en todos los aspectos significativos con la normativa de aplicación.

Los principales incumplimientos incluidos en el informe son:

El SAS no dispone de un procedimiento específico de “Privacidad por Diseño” que garantice que las nuevas iniciativas de tratamiento puedan ser objeto del análisis oportuno por el Delegado de Protección de Datos.

El SAS no tiene formalizada una metodología de análisis de riesgos de privacidad que permita garantizar la identificación, evaluación y gestión de los riesgos de privacidad.

Recomendaciones

Desde la Cámara de Cuentas de Andalucía se recomienda a los responsables de la información y de servicios, así como a los responsables del tratamiento de datos, la adopción de las medidas que se exponen en el informe, en aras a la mejora de la ciberseguridad y de protección de datos.

En cumplimiento de la “Guía práctica para la elaboración de recomendaciones”, aprobada por la Cámara de Cuentas de Andalucía, se ha asignado una prioridad alta o media a cada recomendación, teniendo en cuenta que se trate de una debilidad material o una deficiencia significativa. Las recomendaciones más relevantes se exponen a continuación.

Recomendaciones del Esquema Nacional de Seguridad

Priorizar las actuaciones precisas con el objeto de alcanzar la versión definitiva de la normativa de seguridad del SAS. Esta circunstancia permitirá reforzar y, sobre todo, personalizar las prácticas de actuación que deben ser atendidas por el personal en el uso de los activos de información. (Prioridad alta).

En los procedimientos de seguridad y procesos de autorización, se debieran priorizar las actuaciones necesarias para alcanzar la versión definitiva de la relación de procedimientos de seguridad identificada por el propio SAS. Sólo, de esta forma, se podrá evaluar la efectividad de los procesos de seguridad que conforman el Modelo de Gestión de la Seguridad en el SAS. (Prioridad alta).

CÁMARA DE CUENTAS DE ANDALUCÍA

RESUMEN DE INFORME

Con independencia de que, desde el punto de vista operativo, pueda quedar justificado el mantenimiento de las cuentas de usuarios inhabilitadas, es preciso que la función de Responsable de Seguridad efectúe el análisis de riesgos de seguridad oportunos, para la posible identificación de una estrategia para la mitigación de los riesgos o proceder a la aceptación formal del riesgo por parte del Comité de Seguridad de la Información. (Prioridad media).

Alcanzar la formalización de una política de firma electrónica, así como un procedimiento específico con las pautas de actuación que deben ser atendidas por los profesionales sanitarios en el uso de la firma electrónica. (Prioridad media).

Recomendaciones sobre protección de datos

Alcanzar la formalización del Modelo de Gobierno y Gestión de la Privacidad del SAS, a través del cual, puedan ser atendidas, entre otras, la identificación de los objetivos que conforman la Estrategia de Privacidad del SAS, o el detalle del ciclo de vida operativo asociado a las distintas iniciativas de tratamiento a evaluar. (Prioridad alta).

Formalizar un procedimiento específico con el detalle de las directrices de actuación que deben ser consideradas en cuanto al consentimiento otorgado por el afectado, conforme a la normativa vigente en materia de protección de datos, donde se responda a todas las garantías legales. (Prioridad media).

Aumentar la información y la documentación relacionada con los procesos de tratamiento de datos identificados en el Registro de Actividades de Tratamiento, para que éste actúe como base de datos de las distintas actividades ejecutadas. (Prioridad media).

Formalizar un procedimiento de mantenimiento del Registro de Actividades de Tratamiento a través del cual, se concreten la información y de la documentación que debe acompañar a cada proceso de tratamiento de datos para su inclusión formal en tal registro; la secuencia de actividades asociadas a los procesos de alta, baja y modificación de procesos de tratamiento de datos, y el detalle de las funciones y obligaciones del responsable del tratamiento. (Prioridad media).

NOTA: Los resúmenes se realizan para facilitar la labor de los medios de comunicación y contienen las principales conclusiones del informe. Sin embargo, para realizar un análisis completo de los trabajos de fiscalización de la Cámara de Cuentas es necesario conocer el texto completo del informe que se encuentra en www.ccuentas.es.