DOCUMENTO DE DIRECTRICES TÉCNICAS

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

Ejercicio 2021

(OE 01/2021)

DIRECTRICES TÉCNICAS

1. INTRODUCCIÓN

El Pleno de la Cámara de Cuentas de Andalucía acordó incluir en el Plan de Actuaciones para el año 2021 la realización de un informe denominado "Control de ciberseguridad en determinadas áreas del Servicio Andaluz de Salud (SAS) y sus entidades vinculadas".

Se propone modificar el título del informe a "Auditoría de cumplimiento de ciberseguridad y protección de datos del sistema de receta médica electrónica del Servicio Andaluz de Salud (SAS)". El alcance del informe permite considerar esta fiscalización como una auditoría de cumplimiento de la normativa relativa al Esquema Nacional de Seguridad y a la protección de datos. Además, se tendrán en cuenta la GPF-OCEX 4320 "Guía sobre la importancia relativa en las fiscalizaciones de cumplimiento" y la GPF-OCEX 4000 "Guía para las auditorias de cumplimiento".

En el desarrollo de su función fiscalizadora, la Cámara de Cuentas de Andalucía está facultada para verificar la disponibilidad, integridad, confidencialidad, trazabilidad y autenticación de la información y de los sistemas informáticos que soportan los procesos de las organizaciones. Cada vez un mayor número de aspectos de la gestión pública se realiza con el soporte y apoyo de complejos sistemas, y la conectividad a internet se ha convertido en una característica fundamental de dichos sistemas de información. Esta circunstancia ha traído aparejado un crecimiento de las amenazas de todo tipo, multiplicándose los incidentes de seguridad de los que son víctimas los sistemas de información y comunicaciones de las entidades públicas, con graves repercusiones potenciales, tanto económicas, como en la prestación de los servicios públicos.

En la Guía Práctica de Fiscalización de los OCEX sobre *Ciberseguridad, seguridad de la información y auditoría externa* (GPF-OCEX 5311), se acentúa la importancia de la ciberseguridad para gobiernos, gestores y auditores públicos, debido a la potencial repercusión que las amenazas a la seguridad de los sistemas de información representan, que puede afectar a las cuentas que se auditan y a la continuidad de los servicios públicos.

Esta actuación responde a una línea de actuaciones fiscalizadoras centradas en el control de la transformación digital experimentada por las Administraciones Públicas, y, más concretamente, en el Servicio Andaluz de Salud, debido a la especial protección de la información que se maneja y la importancia del servicio.

En este informe, además del equipo de fiscalización de la CCA, se cuenta con la colaboración de la empresa Techware Consultin&Training, S.L. que posee las certificaciones CISA (Certified Information System Auditor), CDPSE (Certified Data Protection Engineer Solutions), CISM (Certified Information Security Manager), CGEIT (Certified on Government of IT Enterprise), CRISC (Certified in Risk and Information Systems Controls) y CRMA (Certified in Risk Management Assurance).

DIRECTRICES TÉCNICAS

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí, con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas. Asimismo, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados, tal como recoge el Esquema Nacional de Seguridad (ENS) en su artículo 156.

El artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, incluye entre los derechos de las personas, en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en sus ficheros, sistemas y aplicaciones.

La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos (garantías de seguridad de los servicios), que permita a ciudadanos y Administraciones Públicas el ejercicio de los derechos y el cumplimiento de sus deberes a través de estos medios.

Asimismo, el ENS persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiar la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Para la profundización y contribución a un mejor cumplimiento de los mandatos normativos, se clarifica el papel del Centro Criptológico Nacional (CCN) y del CCN-CERT[1], donde se explicita y relacionan las instrucciones técnicas de seguridad, y la declaración de aplicabilidad, en aras a la adecuación de lo previsto en el Reglamento 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 interior.

Al SAS le resulta de aplicación y de obligado cumplimiento el ENS, tal y como se recoge en el artículo 3 del 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.

La necesidad de ofrecer servicios sanitarios públicos de calidad, conforme a los principios de eficiencia, accesibilidad, equidad, uso óptimo de los recursos y satisfacción de los usuarios, conlleva gestionar de manera segura la información. Esto, unido al uso de las tecnologías de la información y comunicaciones (TIC), pone de manifiesto la necesidad de que las entidades

[1] CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

públicas definan sus políticas de seguridad. Para dar respuesta a ello, en el año 2003 se puso en marcha por el SAS, en colaboración con Consejo Andaluz de Colegios Oficiales de Farmacéuticos (CACOF), la receta electrónica, que se denomina Receta XXI. La receta médica y las órdenes de dispensación suponen un medio fundamental para la transmisión de información entre los profesionales sanitarios, y una garantía para el paciente.

La categoría de un sistema de información, en materia de seguridad, modulará 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 criterio del principio de proporcionalidad.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La mencionada categorización de un sistema se realizará de acuerdo con lo establecido en el RD 3/2010 del Esquema Nacional de Seguridad, y será de aplicación a todos los sistemas empleados para la prestación de los servicios del SAS, y soporte del procedimiento administrativo general.

2. OBJETIVOS Y ALCANCE DE LA FISCALIZACIÓN

2.1. Tipo de fiscalización

Por un lado, se trata de una auditoría de cumplimiento de seguridad y protección de datos donde se opinará sobre el grado de cumplimiento del ENS, se identificarán sus deficiencias, y se recomendarán las posibles medidas correctoras o complementarias que sean necesarias.

Por otro, se dará una opinión sobre la protección de datos, más concretamente, con relación al cumplimiento de los principios, derechos y obligaciones recogidas en el marco normativo de aplicación (RGPD y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), identificando deficiencias y proponiendo las medidas correctoras o complementarias que se estimen oportunas.

2.2. Objetivos

La implantación del ENS debe permitir la formalización de la Política de Seguridad en la utilización de los medios electrónicos, con la identificación de los Principios Básicos[2]y Requisitos Mínimos [3]que permitan garantizar la seguridad de los servicios.

Se va a realizar una auditoría de cumplimiento de seguridad y protección de datos con el objetivo de emitir opinión sobre los siguientes objetos:

- Evaluación del cumplimiento del Esquema Nacional de Seguridad (revisión de las medidas de seguridad del Anexo II del ENS).

  El objetivo final es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados. Es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

- Evaluación de la aplicación de la normativa de protección de datos vigente, en el cumplimiento de los principios, derechos y obligaciones recogidas en el mismo, garantizando que los procesos de tratamiento de datos alcancen el cumplimiento del RGPD y de la Ley Orgánica 3/2018 (en adelante protección de datos).

Para ello, se llevará a cabo el trabajo de conformidad con las Guías CCN-STIC, en particular, CCN-STIC 802 - Auditoría de ENS y CCN-STIC 808 - Verificación del cumplimiento de las medidas en el ENS.

En esta misma línea, aprovechando lo expuesto en la Disposición Adicional Primera de la LOPD-GDD[4], se analizará el gobierno de la normativa sobre protección de datos.

Para analizar el cumplimiento de la normativa de protección de datos vigente, se contrastará la identificación e implantación de las medidas técnicas y organizativas para garantizar:

- El cumplimiento de los principios (arts. 5 a 14 del RGPD, así como los que se derivan a tales efectos y queden recogidos en la Ley 3/2018).
- El cumplimiento de los derechos, (arts. 15 a 23 del RGPD, así como los que se derivan a tales efectos y queden recogidos en la Ley 3/2018).
- El cumplimiento de las obligaciones (arts. 24 a 49 del Reglamento General de Protección de Datos, así como los que se derivan a tales efectos y queden recogidos en la Ley 3/2018).

[2] Principios Básicos: Fundamentos que deben ser considerados en el proceso de formalización del Modelo de Gobierno y Gestión de la Seguridad.
[3] Requisitos Mínimos: Detalle de los objetivos de control de obligado cumplimiento para garantizar la seguridad de los servicios.
[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Por último, se utilizará la GPF-OCEX 5312 Glosario de Ciberseguridad y otras Guías prácticas de fiscalización de los Órganos de Control Externo (GPF-OCEX) que resulten de aplicación, así como GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa, ya citada.

2.3. Alcance de la fiscalización

2.3.1. Ámbito subjetivo

El ámbito subjetivo de la presente actuación serán las actuaciones en materia de seguridad y protección de datos llevadas a cabo por el SAS, por lo que la fiscalización debe desarrollarse con las garantías metodológicas y de independencia, profesionalidad y adecuación requerida.

De igual forma, y teniendo en consideración las características de la fiscalización y el ámbito de aplicación de la normativa, quedará identificada como muestra en el alcance de los servicios de auditoría tres farmacias de referencia en el territorio andaluz consideradas por la Cámara de Cuentas de Andalucía a tales efectos.

2.3.2. Ámbito objetivo

Constituyen el **alcance objetivo** el sistema de información Receta XXI, considerado como sistema de categoría media.

Dentro de los trabajos se tendrá en cuenta el cumplimiento de la legislación vigente de seguridad y de protección de datos en todo el alcance recogido por el articulado de las mencionadas normativas.

El entorno de información afectado por la auditoría se circunscribe al conjunto de módulos que componen Receta XXI.

En este sentido, por tanto, la auditoría mantiene como alcance el siguiente conjunto de módulos que integran la Receta XXI:

- Dispensaciones: es el módulo donde se almacena información sobre la medicación prescrita al usuario y las características del tipo de financiación. Desde este módulo, las oficinas de farmacia pueden consultar, modificar y realizar las dispensaciones sobre medicamentos o productos sanitarios anteriormente prescritos por el médico, todo ello previa validación de la tarjeta sanitaria del paciente y autenticación del farmacéutico en el sistema, donde consta la medicación prescrita y las características del tipo de financiación que corresponda al paciente (activo, pensionista, otros).
- Prescripciones: es el módulo desde el cual se gestiona la emisión de las prescripciones y el histórico de las mismas por parte de los profesionales asistenciales.
- Visados: es el módulo que permite gestionar los visados de aquellos medicamentos prescritos en Receta XXI que necesitan de una autorización.

- Control de recetas: es un módulo en el que se registran y almacenan aquellas recetas médicas y órdenes de dispensación oficiales del Sistema Nacional de Salud emitidas en soporte papel, que se le han perdido al prescriptor o le han sido sustraídas.
- Nomenclátor: es el módulo desde el cual se realiza la actualización, inserción y/o modificación de los registros correspondientes al vademécum del SAS, y desde el cual se aplican los filtros sobre los registros del vademécum y se lleva a cabo la programación para ejecutar las actualizaciones sobre los módulos de dispensaciones y prescripciones.
- Gestión de farmacias: es el módulo encargado de gestionar los datos y perfiles de las oficinas de farmacias.

Se dará cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, el Real Decreto 951/2015, de 23 de octubre, por el que se regula el ENS en el ámbito de la Administración Electrónica en cuanto a la materia de seguridad, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, circunscribiendo su análisis del servicio de Receta XXI y las farmacias que lo utilizan como servicio.

Las medidas de seguridad a auditar pueden abarcar medidas de naturaleza diversa (organizativa, física y lógica, entre otras). Por lo tanto, se identifican los elementos que entran dentro de ésta:

- En materia de seguridad, se analizará las medidas de seguridad del Anexo II del RD 3/2010, salvo que la exclusión de alguna de ellas haya quedado debidamente justificada en la Declaración de Aplicabilidad emitida a tales efectos. En particular, se tendrá en cuenta:
    - El marco organizativo del SAS.
    - El marco operacional del SAS y, por extensión, su aplicación en las farmacias.
    - Las medidas de protección de Receta XXI, y, por extensión, su aplicación en las farmacias.

- En cuanto a la protección de datos, se comprobará el cumplimiento de los principios, derechos y obligaciones de aplicación en el contexto de Receta XXI, y por extensión, su aplicación en las farmacias.

Se trata de un compromiso de atestiguamiento donde la parte responsable, en este caso, el SAS mide la materia en cuestión, de acuerdo con los criterios y presenta la información de la materia, sobre la que el equipo de auditoría procederá a reunir evidencia de auditoría suficiente y apropiada para obtener una base razonable que permita expresar una opinión.

La auditoría de cumplimiento de seguridad y protección de datos llevada a cabo se realiza con una seguridad razonable de que la política de seguridad del SAS en relación con la receta electrónica "Receta XXI" resulten, en todos los aspectos significativos, conforme a la normativa del ENS y de protección de datos.

2.3.3. Alcance temporal

En cuanto al ámbito temporal de la fiscalización será referido al ejercicio 2021, donde se aplicarán procedimientos de auditoría sobre ejercicios anteriores y posteriores en caso de resultar necesario respecto al cumplimiento de ciberseguridad del ENS y del cumplimiento de protección de datos.

2.4. Metodología

2.4.1. Planificación y trabajo de campo

Para la realización de la auditoría, la metodología utilizada debe permitir comprobar, a través de los registros y evidencias de auditoría, las limitaciones que se hayan podido producir en el desarrollo de las tareas, y las actividades realizadas.

La evolución que ha seguido Receta XXI desde su implantación se muestra en el cuadro nº1

EVOLUCIÓN RECETA XXI

AÑO	Recetas Totales	Nº de Recetas XXI	% Recetas XXI
2004	137.011.368	247.315	0%
2005	141.263.195	1.245.313	1%
2006	147.639.901	8.982.319	6%
2007	156.831.096	30.517.813	19%
2008	166.986.378	66.315.635	40%
2009	177.371.672	89.240.783	50%
2010	180.189.079	105.485.676	59%
2011	182.549.119	119.184.695	65%
2012	172.960.149	138.868.831	80%
2013	162.156.738	153.744.375	95%
2014	165.040.914	158.614.180	96%
2015	167.369.136	161.979.043	97%
2016	169.950.601	165.698.229	97%
2017	171.535.695	168.409.009	98%
2018	176.064.083	173.315.231	98%
2019	181.574.645	179.323.500	99%
2020	184.678.800	183.257.532	99%
2021	195.082.041	193.893.258	99%

Cuadro nº 1

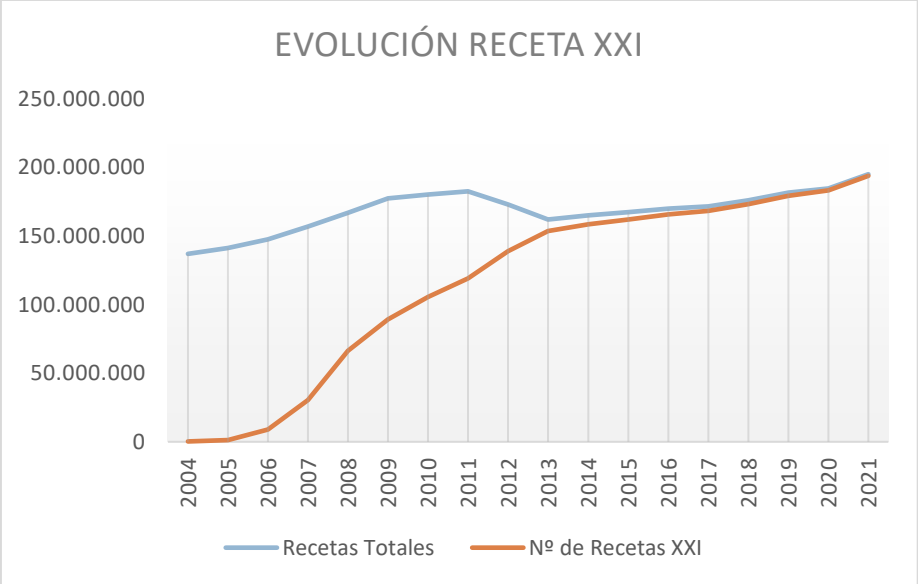


Gráfico nº1

En primer lugar, se realizarán una serie de cuestionarios para conocer los sistemas informáticos, mediante los que se gestiona la prescripción y dispensación de medicación (no hospitalaria) Receta XXI, de forma que se pueda evaluar el cumplimiento del ENS y la normativa de protección de datos vigente.

La metodología de auditoría empleada mantendrá como referencia prioritaria la aplicación de las buenas prácticas formalmente reconocidas en materia de auditoría de TI y, con carácter general, para la función de auditoría interna, esto es:

- Metodología de auditoría de TI emitida por ISACA *(Information Systems Audit and Control Association)*, para las tareas de aseguramiento y revisión del sistema de control interno considerado para los sistemas de información y, con carácter general, la infraestructura de TI (hardware, software, comunicaciones, soportes, instalaciones y usuarios).
- Disposiciones recogidas en el Marco Internacional para la Práctica Profesional de la Auditoría Interna emitidas por el IIA *(Institute of Internal Auditors)*.
- Guía CCN-STIC-802 de auditoría del ENS para la atención de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de Seguridad) del ENS.

La metodología aplicada mantendrá, como objetivo principal, ayudar a identificar aquellos escenarios de incumplimiento por parte del sistema de información Receta XXI, comprendido en el ámbito de aplicación según dispone el artículo 3 del ENS, así como facilitar la emisión de un informe con el detalle de las no conformidades existentes a este respecto. De igual forma, se incluirán las recomendaciones que se consideran apropiadas, como estrategia de mitigación del riesgo para garantizar el cumplimiento normativo oportuno.

DIRECTRICES TÉCNICAS

Esta metodología, manteniendo como marco de referencia, los objetivos de control y cumplimiento legal establecidos en el ENS tendrá en cuenta las siguientes consideraciones:

- La evaluación de riesgos inherentes a las tecnologías de la información desplegadas, y a los procesos existentes para el tratamiento de los datos de carácter personal.
- La ejecución de las pruebas necesarias para evidenciar si las medidas técnicas y organizativas demandadas según Declaración de Aplicabilidad y Anexo II del ENS se cumplen en el tiempo, y de forma consistente.

  Las evidencias obtenidas con el objeto de proporcionar garantías suficientes en lo relativo a la correcta implantación de las medidas técnicas y organizativas de seguridad identificadas, podrán ser el resultado de la utilización de cuatro técnicas diferentes de auditoría:

  a) Entrevistas-testimonios obtenidos en el transcurso de las reuniones de trabajo planificadas.

  b) Documentos formalmente emitidos en el contexto del cuerpo normativo de seguridad o en el ámbito de la protección de datos de carácter personal.

  c) Observaciones realizadas por el equipo auditor durante la auditoría in situ, si procede.

  d) Resultado de las pruebas específicas efectuadas por el equipo de auditoría en presencia de los auditados.

Se identifican las siguientes líneas de actuación:

- La investigación preliminar se centra en la revisión de la documentación previa solicitada, así como la planificación de reuniones con los principales interlocutores con el objeto de alcanzar una primera percepción del ambiente de control interno existente.
- La elaboración y ejecución de los programas de auditoría con la identificación de las pruebas de auditoría consideradas oportunas a tales efectos.

  En el ámbito de la auditoría relativa al ENS serán atendidas las consideraciones planteadas en la guía CCN-STIC 802.
- La emisión del Informe de Auditoría con la exposición de las posibles no conformidades identificadas y evidenciadas como resultado de la ejecución del programa de trabajo, así como la presentación del detalle de las posibles acciones preventivas o correctivas que permiten la mitigación de las situaciones de riesgo de seguridad que pudieran derivarse.

Estas evidencias serán debidamente referenciadas en los papeles de trabajo, siendo custodiadas por el equipo de auditoría.

La GPF-OCEX 1301 "Guía sobre la planificación de una fiscalización" propone como anexo a las directrices técnicas, adjuntar el programa de trabajo. Se depositarán en el espacio previsto en la intranet de la CCA.

2.4.2. Hallazgos

El objetivo principal de la presentación de los resultados de las revisiones y pruebas, antes de la emisión del informe de auditoría, es confirmar los hechos y las situaciones detectadas o identificadas como resultado de las pruebas y revisiones realizadas.

Para la evidencia obtenida, se procederá:

- Si no hay incidencias a comunicar, se acreditará la realización adecuada de la prueba y sus resultados.
- Si hay hallazgos de no conformidad a incluir en el informe, se evidenciará claramente el incumplimiento persistente o una indiscutible deficiencia de seguridad, y no aquellas situaciones excepcionales o puntuales, si están reportadas, controladas, y aprobadas, a menos que la excepcionalidad no debiera haber sido aprobada, por el riesgo que pudiera implicar, según el juicio objetivo y sustentado del auditor.

3. CONOCIMIENTO DEL SISTEMA DE INFORMACIÓN RECETA XXI DEL SERVICIO ANDALUZ DE SALUD Y SU ENTORNO

3.1. Naturaleza y objeto

DIRAYA es el nombre con el que se conoce al conjunto de sistemas de información que se utilizan en el SAS como soporte de la información y gestión de la atención sanitaria. DIRAYA integra toda la información de cada usuario del sistema público de salud, con independencia del profesional o ámbito asistencial que la genere, en una historia de salud única, disponible dónde y cuándo sea preciso para su atención, facilitando así la accesibilidad a los servicios y mejorando las prestaciones del sistema sanitario.

Receta XXI es el sistema de receta electrónica de DIRAYA, nombre con el que se conoce al conjunto de sistemas de información que se utilizan en el Servicio Andaluz de Salud como soporte de la información y gestión de la atención sanitaria.

El sistema facilita la prescripción y el control de los medicamentos por parte de los profesionales asistenciales, que pueden consultar medicaciones pasadas y actuales en la historia de salud única. A su vez, los farmacéuticos pueden acceder a los datos sobre prescripción, comprobar la medicación que han de dispensar, anotar los medicamentos entregados e incluso informar al médico de cualquier incidente.

Receta XXI gestiona un número muy elevado de recetas, y tiene a los distintos agentes participantes en la gestión repartidos a lo largo de todo el territorio de Andalucía

(profesionales asistenciales, farmacias, pacientes, etc.), por lo que precisa del soporte de unos potentes y complejos sistemas de información que ofrezcan un grado de fiabilidad y disponibilidad muy elevado. Es, por tanto, totalmente dependiente de las tecnologías de la información y las comunicaciones, y la ciberseguridad frente a crecientes y sofisticadas amenazas al conjunto del sistema y la capacidad de recuperación de estos sistemas frente a potenciales incidentes, accidentales o intencionados, son aspectos muy relevantes que deben ser considerados al diseñar los controles que garanticen su adecuado funcionamiento.

Implementa un modelo de prescripción y dispensación de los medicamentos y productos sanitarios incluidos en la financiación pública que, aprovechando las posibilidades de la actual tecnología informática y de telecomunicaciones, aporta ventajas respecto a la prescripción tradicional de recetas en papel. Cuando el profesional realiza la prescripción de un medicamento o producto sanitario a un paciente a través del módulo de prescripciones, esta se almacena en la base de datos de prescripciones y determinados datos de dicha prescripción son enviados y grabados en la base de datos de dispensación. En este módulo, para ese paciente, identificado previamente en la base de datos de usuarios del Sistema Sanitario Público de Andalucía, se creará un crédito farmacéutico con el tratamiento completo prescrito para su médico/enfermero.

El conjunto de los productos prescritos se imprimirá en una hoja informativa para el paciente, en la que el profesional, además de los datos obligados de posología y duración del tratamiento, podrá incluir las instrucciones que considere necesarias. Esta hoja informativa será custodiada por el paciente, de forma que pueda presentarla en las sucesivas dispensaciones hasta su caducidad.

Para la dispensación de los productos prescritos por el profesional, el paciente se dirigirá a una oficina de farmacia. En dicho establecimiento debe presentar su tarjeta sanitaria como medio de autentificación y como dispositivo que servirá al farmacéutico, debidamente acreditado por el SAS, para acceder, vía web, al módulo de dispensaciones, donde consta la medicación prescrita y las características del tipo de financiación que corresponda al paciente (activo, pensionista, otros).

El farmacéutico realizará la dispensación siguiendo la pauta establecida. El profesional prescriptor, en cualquier momento, podrá modificar o anular los registros de la prescripción que estime necesarios, informando de ello a su paciente. Asimismo, podrá consultar las dispensaciones que se vayan realizando a sus pacientes. Cuando causas asistenciales lo aconsejen, el farmacéutico podrá bloquear, de forma cautelar, la dispensación de una prescripción concreta. El sistema enviaría en este caso una alerta al buzón del profesional informando de ello, y en el histórico del tratamiento se reflejará la anulación.

3.2. Normativa de aplicación

El marco jurídico que engloba esta materia y en la que se basa el equipo de auditoría para la realización de su trabajo es la siguiente.

- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
- Reglamento (UE) 2016/679 del Parlamento Europeo Y del Consejo de 27 de abril de 2016 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
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Decreto 181/2007, de 19 de junio, por el que se regula la receta médica electrónica.
- Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.
- Resolución de 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se aprueba la Política de Seguridad de las Tecnologías de la información y la comunicación del Servicio Andaluz de Salud.
- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

También se observará las guías del CCN-STIC:

- Guía CCN-STIC 809 Declaración y Certificación de Conformidad con el ENS
- Guía CCN-STIC-802 Auditoría del ENS
- Guía CCN-STIC-804 ENS. Guía de implantación
- Guía CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS
- Guía CCN-STIC 824 Informe del Estado de Seguridad

4. INFORME A EMITIR

Se emitirá un Informe de cumplimiento del ENS y de protección de datos, donde se expresarán dos opiniones independientes sin tener en consideración la Disposición Adicional Primera de la Ley Orgánica 3/2018[5], para no condicionar la opinión sobre protección de datos al ENS. Asimismo, se detallará el cumplimiento de cada medida indicada en el Anexo II del ENS según la categorización del SAS para este sistema de información (con arreglo al Anexo I del ENS), la evidencia en caso de incumplimiento para subsanar esta situación.

Asimismo, dicho informe de cumplimiento recogerá los principios, derechos y obligaciones formalizados a través del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD – Reglamento General de Protección de Datos), 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, aplicable desde el 25 de mayo de 2018, así como la Ley Orgánica, 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantías de los Derechos Digitales (Ley 3/2018), aplicable desde el 6 de diciembre de 2018, en el contexto de los procesos de tratamiento de datos personales afectados por los sistemas de información que sustentan RECETA XXI.

La estructura de informe seguirá los modelos de informe para fiscalizaciones de cumplimiento de legalidad contenidos en el anexo I de la GPF- OCEX 4000" Las fiscalizaciones de cumplimiento de legalidad y modelos de informe", en función de las salvedades y del tipo de opinión que se formule:

1. INTRODUCCIÓN
2. RESPONSABILIDAD DE LOS ÓRGANOS GESTORES DE LA ADMINISTRACIÓN
3. RESPONSABILIDAD DE LA CÁMARA DE CUENTAS DE ANDALUCÍA
4. OPINIÓN
4.1 Opinión ENS
4.2 Opinión sobre protección de datos
5. FUNDAMENTO DE LA OPINIÓN
5.1 Fundamentos de la opinión ENS
5.2 Fundamentos de la opinión sobre protección de datos
6. OTROS ASPECTOS QUE NO AFECTAN A LA OPINIÓN
7. RECOMENDACIONES
8. APÉNDICES
9. ANEXOS
10. ALEGACIONES

[5] Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.
1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.
2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.
En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Además del informe correspondiente, se emitirá un documento interno donde se detallarán los hallazgos de no conformidad y que por razones de seguridad el equipo de auditoría no entregará ni concederá acceso al mismo a terceros distintos del responsable de seguridad y el responsable de protección de datos, salvo por imperativo legal o mandato judicial.

5. EQUIPO DE AUDITORÍA, PRESUPUESTO DE TIEMPO Y CALENDARIO PREVISTO

5.1. Equipo de auditoría

El consejero del departamento que asume la dirección de la fiscalización es Antonio M. López Hernández.

El equipo de auditoría está compuesto por un Coordinador de Departamento, un técnico informático, un técnico de auditoría y un administrativo.

5.2. Presupuesto de tiempo

La estimación de horas de trabajo de la presente actuación es la siguiente:

MES	AÑO	DIAS LAB.	HORAS MES	HORAS JEFE EQUIPO	HORAS TÉCNICO	HORAS INFORMÁTICA	HORAS EXTERNO*	TOTAL HORAS
				Horas	Horas	Horas	Horas	Horas
Enero	**2022**	11	77	-	-	38,5	24	**62,50**
Febrero	**2022**	19	133	15	66,5	66,5	40	**188,00**
Marzo	**2022**	23	161	15	80,5	80,5	48	**224,00**
Abril	**2022**	19	125,5	15	125,5	62,75	80	**283,30**
Mayo	**2022**	20	132,5	10	132,5	66,25	80	**288,80**
Junio	**2022**	22	154	50	154	77	-	**281,00**
Julio	**2022**	21	147	50	147	73.5		
Septiembre	**2022**	20	140	50	140	70		
TOTALES:	-	**114**	**783**	**205**	**846**	**535**	**272**	**1.858**

*Las jornadas de la empresa externa constan de 8 horas/día.

5.3. Calendario previsto

El calendario previsto[6] para la presente actuación se detalla a continuación:

FASES	FECHAS
Inicio de la planificación	17/11/2021
Inicio de los trabajos de campo	17/01/2022
Finalización de la planificación (DT)	20/04/2022
Finalización de los trabajos de campo	15/07/2022
Elaboración del Borrador del Informe	15/09/2022
Entrega al Consejero	28/09/2022

[6] La previsión de fechas en el trabajo puede verse alterada por el retraso en la entrega de información por el SAS.