3. Otras disposiciones

CÁMARA DE CUENTAS DE ANDALUCÍA

Resolución de 27 de julio de 2023, de la Cámara de Cuentas de Andalucía, por la que se ordena la publicación del Informe de Auditoría de cumplimiento de ciberseguridad y protección de datos del sistema de receta médica electrónica del Servicio Andaluz de Salud (SAS). Ejercicio 2021.

En virtud de las facultades que me vienen atribuidas por el artículo 21 de la Ley 1/1988, de 17 de marzo, de la Cámara de Cuentas de Andalucía, y del Acuerdo adoptado por el Pleno de esta Institución, en la sesión celebrada el 20 de junio de 2023,

R E S U E L V O

De conformidad con el art. 12 de la citada Ley 1/1988, ordenar la publicación del Informe de Auditoría de cumplimiento de ciberseguridad y protección de datos del sistema de receta médica electrónica del Servicio Andaluz de Salud (SAS), correspondiente al ejercicio 2021.

Sevilla, 27 de julio de 2023.- La Presidenta, Carmen Núñez García.

AUDITORÍA DE CUMPLIMIENTO DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS DEL SISTEMA DE RECETA MÉDICA ELECTRÓNICA DEL SERVICIO ANDALUZ DE SALUD (SAS). EJERCICIO 2021

El Pleno de la Cámara de Cuentas de Andalucía, en su sesión celebrada el día 20 de junio de 2023, con la asistencia de todos sus miembros, ha acordado aprobar el Informe de Auditoría de cumplimiento de ciberseguridad y protección de datos del sistema de receta médica electrónica del Servicio Andaluz de Salud (SAS), correspondiente al ejercicio 2021.

Í N D I C E

00287890

ABREVIATURAS Y SIGLAS

Bia:	Análisis de Impacto en el Negocio.
Cacof:	Consejo Andaluz de Colegios Oficiales de Farmacéuticos.
CCA	Cámara de Cuentas de Andalucía.
CCN	Centro Criptológico Nacional.
CSISTIC	Comité de Seguridad Interior y Seguridad TIC.
CSISTIC-SAS	Comité de Seguridad Interior y Seguridad TIC del SAS.
ENS	Esquema Nacional de Seguridad.
ICEX	Instituciones de Control Externo.
IIA	Institute of Internal Auditors.
ISACA	Information Systems Audit and Control Association.
LOPDPGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
OCEX	Órgano de Control Externo.
PIA	Análisis de Impacto de Privacidad.
RAT	Registro de Actividades de Tratamiento.
RGPD	Reglamento General de Protección de Datos.
SAS	Servicio Andaluz de Salud.
TI	Tecnología de la información.
TIC	Tecnología de la Información y Comunicación.
UE	Unión Europea.

00287890

1. INTRODUCCIÓN

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

2 La fiscalización de cumplimiento sobre ciberseguridad y protección de datos, inicialmente configurada como una fiscalización sobre controles de ciberseguridad, abre una nueva línea de actuaciones por parte de la Cámara de Cuentas de Andalucía (CCA) encaminada a la verificación del cumplimiento del Esquema Nacional de Seguridad (ENS) y de protección de datos.

3 El artículo 18 de la Constitución Española prevé, específicamente, que se garantizará el secreto de las comunicaciones y se limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

4 A su vez, el Estatuto de Autonomía para Andalucía (Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía), propugna en su capítulo II del título I el derecho al acceso a las tecnologías de la información y de la comunicación, y a participar activamente en la sociedad del conocimiento, la información y la comunicación.

5 De manera más concreta, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, sienta las bases necesarias de seguridad en el uso de los medios electrónicos.

6 Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Por tanto, la finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de 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.

7 El ENS se aplica a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre; a los sistemas que tratan información clasificada, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales; y 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.

8 Ante estas medidas de seguridad, condicionadas al nivel de seguridad en cada dimensión (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.

9 La normativa expone la necesidad de realizar una auditoría del ENS ya sea el sistema catalogado como básico, medio o alto cada dos años o cuando se produzcan modificaciones sustanciales en el sistema.

00287890

10 Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPGDD), ordenó, en su disposición adicional primera, que dichas medidas de seguridad se implantasen 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, 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, por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

11 De otra parte, la citada disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público, y a las del sector privado que colaboren con estas en la prestación de servicios públicos, que involucren el tratamiento de datos personales.

12 Las categorías del ENS establecen las medidas mínimas a cumplir, y se determinan por el impacto que tenga un incidente de seguridad en relación con la organización y las cinco dimensiones que establece (Integridad, confidencialidad, trazabilidad, autenticidad y disponibilidad). Mientras que las medidas específicas que requiere la protección de los datos de carácter personal tienen su origen en el análisis de riesgo correspondiente.

13 Es por ello por lo que cada sistema de información debe evaluarse independientemente tanto para su conformidad con la normativa de protección de datos, como para lo establecido en el ENS.

14 Al SAS le resulta de aplicación y de obligado cumplimiento el ENS, tal y como se recoge en el artículo 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

15 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 como un activo de gran importancia. Esto, unido al uso cada vez mayor de las tecnologías de la información y comunicaciones (TIC), ponen de manifiesto la necesidad de definir la política de seguridad TIC del SAS, con el objetivo de establecer una serie de directrices básicas y perdurables para una protección eficaz de los sistemas gestionados por el organismo, y de la información que se almacena en ellos.

16 Dentro de esa necesidad y del uso cada vez más creciente de las TIC, en el año 2003 se pone en marcha por el Servicio Andaluz de Salud (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.

17 A este respecto el conjunto de módulos que componen RECETA XXI son:

00287890

• 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.

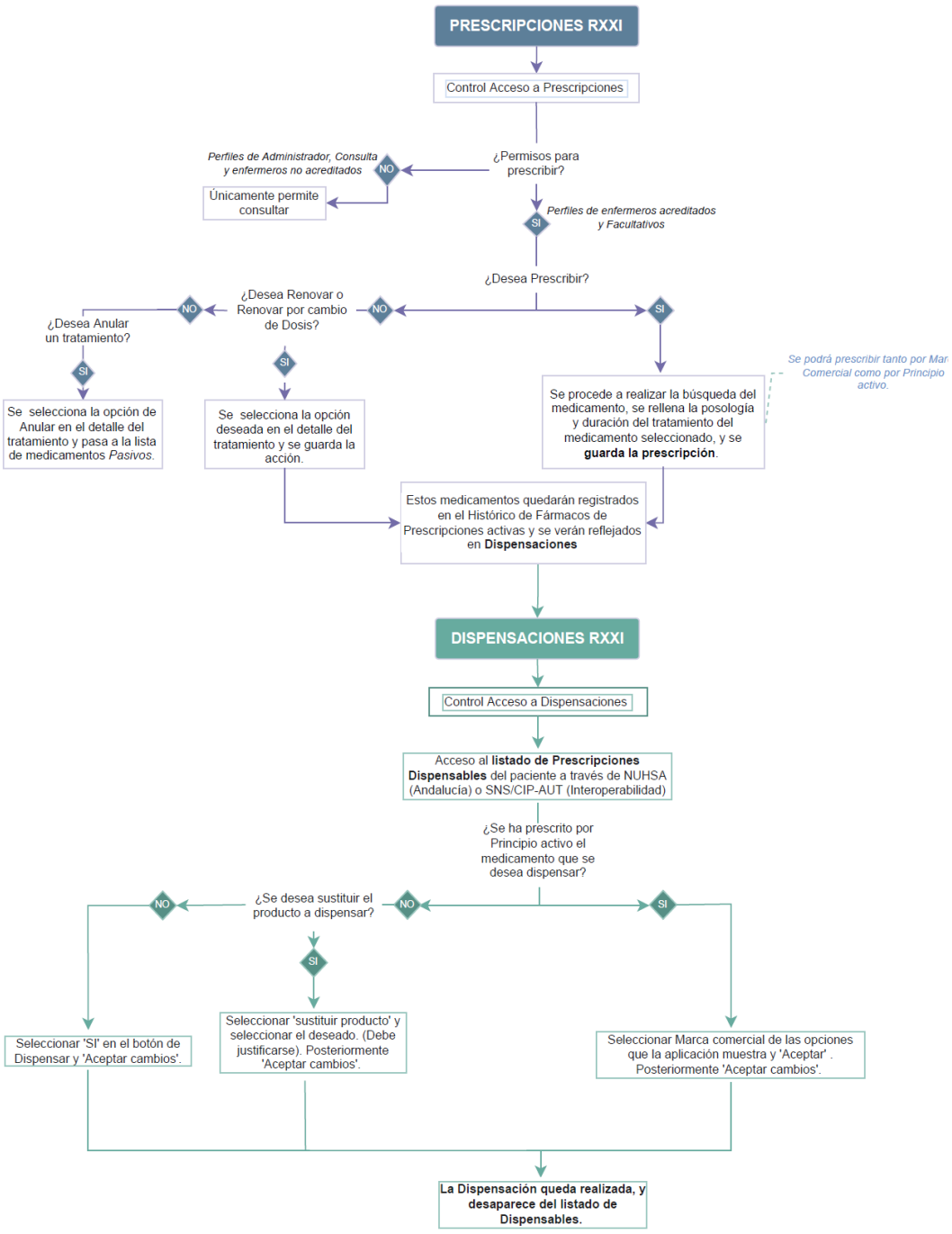
• Control de recetas: es un módulo en el que se registran y almacenan aquellas recetas médicas y órdenes de dispensación oficiales del Sistema Nacional de Salud emitidas en soporte papel, que se le han perdido al prescriptor o le han sido sustraídas.

• Nomenclator: 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.

18 El flujograma, expuesto en el gráfico nº1, describe la iteración entre los diferentes módulos de RECETA XXI:

00287890



FUENTE: Servicio Andaluz de Salud.

Gráfico nº 1

00287890

2. RESPONSABILIDAD DE LOS ÓRGANOS GESTORES DE LA ADMINISTRACIÓN CON RELACIÓN AL CUMPLIMIENTO DE LA LEGALIDAD EN MATERIA DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

19 la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, amplía el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las Administraciones Públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos.

20 Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

21 Por su parte, el SAS, creado mediante la Ley 8/1986, de 6 de mayo, es una agencia administrativa de las previstas en el artículo 65 de la Ley 9/2007, de 22 de octubre de la Administración de la Junta de Andalucía. Está adscrito a la Consejería de Salud y Consumo.

22 El SAS, en tanto que operador crítico del Sistema Nacional de Protección de Infraestructuras críticas, al amparo de lo establecido en la Ley 8/2011, de 28 de abril, de protección de infraestructuras críticas y en el Reglamento de Protección de Infraestructuras críticas aprobado por Real Decreto 704/2011, de 20 de mayo, acomodará sus actuaciones en materia de seguridad interior de sus infraestructuras críticas a lo previsto en estas normas y en las disposiciones de desarrollo de las mismas.

23 Para ello, se crea el Comité de Seguridad Interior y Seguridad TIC del SAS (CSISTIC-SAS) por Resolución de 26 de marzo de 2021 del Director Gerente del Servicio Andaluz de Salud, siendo el órgano de dirección para la Política de Seguridad interior de la Agencia.

3. RESPONSABILIDAD DE LA CÁMARA DE CUENTAS DE ANDALUCÍA EN RELACIÓN CON LA AUDITORÍA

24 La Cámara de Cuentas de Andalucía asume 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.

00287890

25 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[1] "Glosario de Ciberseguridad" y GPF-OCEX 5313 "Revisión de los controles básicos de ciberseguridad".

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.

26 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.

27 El alcance temporal de la fiscalización se ha referido al ejercicio 2021.

28 La metodología que se ha seguido durante el transcurso de la fiscalización se recoge en el apéndice 8.1. Como objetivo principal tanto de la fiscalización como el aplicado en la metodología, en relación con el ENS es 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 del informe con el detalle de las no conformidades, observaciones y/u oportunidades de mejora existentes a este respecto. De igual forma, han sido detalladas las recomendaciones que se consideran apropiadas como estrategia de mitigación del riesgo para garantizar el cumplimiento normativo oportuno.

Por lo que respecta a la protección de datos, se pretende identificar los incumplimientos con relación a los datos personales, en el contexto de los procesos de tratamiento de datos afectados por el sistema de información RECETA XXI. Así mismo, detallar las no conformidades que puedan existir a este respecto. De igual forma, se incorporan las recomendaciones que se consideran apropiadas como estrategia de mitigación del riesgo, para garantizar el cumplimiento normativo oportuno.

29 Constituyen el alcance objetivo el sistema de información Receta XXI, considerado como sistema de categoría media. De acuerdo con el apartado 3. "Determinación del nivel requerido en una dimensión de seguridad" del Anexo I "Categorías de los sistemas" del ENS, se categoriza un sistema de información como categoría de nivel medio 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.

En esta categorización se tiene en cuenta:

[1] Los términos más utilizados en el presente informe se recogen en el Anexo 9.1. "Glosario de términos".

00287890

- 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: Alcanzar sus objetivos, proteger los activos a su cargo, cumplir sus obligaciones diarias de servicio, respetar la legalidad vigente y/o respetar los derechos de las personas.

- 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: Disponibilidad, autenticidad, integridad, confidencialidad, y trazabilidad.

30 Dentro de los trabajos 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.

31 De igual forma, y teniendo en consideración las características de RECETA XXI, así como su ámbito funcional de actuación, los trabajos de auditoría han sido ampliados con el objeto de 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 como usuarios del entorno de información de RECETA XXI.

32 La fiscalización de cumplimiento se ha centrado en la obtención de evidencia suficiente, adecuada y pertinente sobre el cumplimiento, en todos los aspectos significativos, del marco normativo aplicable al ENS y a protección de datos.

33 El objetivo ha sido opinar, en términos de seguridad razonable, sobre si 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 aplicable. En el apéndice 8.2 se recoge la actividad desarrollada para el cumplimiento de objetivos, en el marco de la auditoria.

34 En concreto, el objeto de la auditoría en el ámbito del ENS y Protección de Datos, queda focalizado en la emisión del Informe de Cumplimiento ENS y de protección de datos según el detalle de módulos de RECETA XXI considerado en el alcance de la auditoría, con la exposición del grado de cumplimiento alcanzado para las distintas medidas de seguridad formalizadas a través del Anexo II del ENS, según categorización del sistema efectuada por el SAS con arreglo al Anexo I del ENS, para las distintas dimensiones de seguridad (autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de la información). Así como la exposición del grado de cumplimiento alcanzado para los principios, derechos y obligaciones identificados en el marco normativo considerado de aplicación en materia de protección de datos personales.

35 Los trabajos de campo finalizaron el 30 de septiembre de 2022.

36 Para la realización del trabajo, de acuerdo con la Resolución de 31 de diciembre de 2020 de la CCA, se ha contado con la colaboración de Techware, Consulting & Training, S.L, asumiendo la institución la dirección y supervisión, así como parte de la ejecución de los trabajos. La CCA ha elaborado el presente informe sobre la base del trabajo realizado por la sociedad de auditoría.

00287890

37 Además del informe público, se emiten dos documentos internos donde se detallan los hallazgos de no conformidad, y que, por razones de seguridad, el equipo de auditoría no entrega ni concede acceso al mismo a terceros distintos del responsable de seguridad y el responsable de protección de datos, salvo por imperativo legal o mandato judicial.

4. INFORME DE CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

4.1. Opinión con salvedades

38 En opinión de la Cámara de Cuentas de Andalucía, excepto por los incumplimientos descritos en el apartado "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.

4.2. Fundamentos de la opinión con salvedades del ENS[2]

39 En el apéndice 7.3 "*Cuadro resumen pruebas y evidencias del ENS"* se recoge un resumen de las 75 medidas del Anexo II del ENS, con indicación de la dimensión a la que afecta cada medida, categoría, así como el número de pruebas realizada y el número de evidencias.

40 Para más información, en el apéndice 7.4 "*Cuadro resumen medidas de seguridad del ENS*" se recoge un cuadro resumen de las medidas de seguridad del Anexo II del ENS, indicando su conformidad, observaciones o no conformidades menores. Estas últimas son las salvedades que se indican a continuación.

Marco Operacional

- *Medidas de seguridad: control de acceso*

41 Se incumple la medida 4.2.1 "Identificación [op.acc.1][3]" que exige la singularidad de dicho identificador 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 recibe y qué derechos de acceso recibe, y quién ha hecho algo y qué ha hecho. En este caso, se ha detectado el uso compartido de cuentas de usuario.

42 Atendiendo a lo dictado en la medida 4.2.5 "Mecanismo de autenticación [op.acc.5]" los mecanismos de autenticación frente al sistema pueden usar diferentes factores de autenticación[4] y las exigencias son determinadas por la categoría del sistema. Se ha comprobado que no se ha implementado el doble factor de autenticación siendo una exigencia de la categoría media.

43 La medida 4.2.6 "Acceso local [op.acc.6]" describe las medidas de seguridad que deben ser aplicadas a los puestos de trabajo y que están estratificadas por categoría. En el nivel medio, se

[2] Apéndice 8.3 "*cuadro resumen medidas de seguridad*".
[3] Se utiliza la nomenclatura del Anexo II del RD 3/2010 del ENS, esto es el número y denominación del artículo seguido del código identificativo de la medida de protección entre corcheas.
[4] 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).

00287890

ordena informar al usuario del último acceso efectuado con su identidad, cosa que se ha verificado que no sucede, por lo que se incumple dicha medida.

- *Medidas de seguridad: monitorización del sistema*

44 La medida 4.6.2 "Sistema de métricas [op.mon.2]" dispone que se deben recopilar los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35 del ENS; y para la categoría media, deberán añadir la recolección de datos para valorar el sistema de gestión de incidentes. El SAS no tenía implementada dicha medida.

Medidas de protección

- *Medidas de seguridad: Protección de infraestructuras e instalaciones.*

45 Se ha verificado que existen accesos no protegidos completamente tal como obliga la medida 5.1.1 "Áreas separadas y con control de acceso [mp.if.1] "que establece que se controlarán las entradas a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas".

- *Medidas de seguridad: Protección de equipos.*

46 A tenor de lo requerido por la medida 5.3.2 "Bloqueo de puesto de trabajo [mp.eq.2]" los equipos deberán bloquear sus pantallas transcurrido un cierto tiempo de inactividad, impidiendo su utilización por personas no autorizadas. Esta medida no está implantada en la actualidad.

5. INFORME DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS

5.1. Opinión con salvedades

47 En opinión de la Cámara de Cuentas de Andalucía, excepto por los incumplimientos descritos en el apartado "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.

5.2. Fundamento de la opinión con salvedades de Protección de Datos

48 En el apéndice 7.6 "*Cuadro resumen pruebas y evidencias del RGPD*" se recoge un resumen de los principios sobre Protección de Datos, con indicación del número de pruebas realizadas y el número de evidencias.

49 Asimismo, en el apéndice 7.7 "*Cuadro resumen de incumplimientos del RGPD*" se recoge un cuadro resumen de los principios sobre Protección de Datos, indicando el artículo que se incumple y el tipo de incumplimiento, siendo estos los que se indican a continuación.

50 Tras analizar la documentación aportada por el SAS en materia de protección de datos, no se identifica ningún documento específico a través del cual se determinen las directrices, criterios de actuación y metodologías de trabajo que serán atendidas para garantizar, en sentido estricto, el cumplimiento de principios, derechos y obligaciones en el contexto de los distintos procesos de

00287890

tratamiento de datos existentes en el ámbito del SAS manteniendo un enfoque orientado a la gestión de los riesgos de privacidad. Por lo tanto, se trata de un incumplimiento de los artículos 5.2 y 24.2 del RGPD.

51 Incumpliendo el artículo 25.1 de la RGPD, 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 de privacidad oportuno por parte del Delegado de Protección de Datos para el cumplimiento de los principios, derechos y obligaciones demandados por la actual normativa de protección de datos.

52 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 en el contexto de los distintos procesos de tratamiento de datos identificados en el Registro de Actividades de Tratamiento, incumpliendo el artículo 24.1 del RGPD.

53 No se han formalizado los criterios para determinar la necesidad de ejecutar la evaluación de impacto de privacidad, que garantice el cumplimiento del Principio de Privacidad por Diseño, por lo que se incumple el artículo 35 del RGPD, con las siguientes consecuencias:

- No poder garantizar que se han seguido criterios comunes ante las evaluaciones de impacto de privacidad de los procesos de tratamiento de datos identificados en el Registro de Actividades de Tratamiento.
- Son necesarios para cualquier nueva iniciativa de tratamiento.

6. RECOMENDACIONES

54 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 expuestas en este punto, en aras a la mejora de la ciberseguridad y de protección de datos[5]. En cumplimiento de la "Guía práctica para la elaboración de recomendaciones", elaborada por la Cámara de Cuentas de Andalucía, se ha asignado una prioridad alta o media a cada recomendación, teniendo en cuenta si se trata de una debilidad material o una deficiencia significativa. En el caso de una prioridad alta, se requiere atención urgente de la dirección para implantar controles/procedimientos que mitiguen los riesgos identificados en forma de conclusiones. Para una prioridad media, la dirección deberá establecer un plan de acción concreto para resolver la deficiencia observada en un plazo razonable. Al final de cada recomendación se concreta la prioridad asignada. Las recomendaciones son las que se exponen a continuación:

6.1. Recomendaciones del ENS

55 De acuerdo con el principio de proporcionalidad, los incumplimientos leves o poco significativos, equivalentes a observaciones en el ámbito de ENS, se plasman como recomendaciones, al no considerarse salvedades. De tal forma que se priorizan en función de su pertenencia a los diferentes grupos de medidas del Anexo II del ENS. Siendo de prioridad alta las que se encuentren dentro del

[5] Punto modificado por la alegación presentada.

00287890

marco organizativo, prioridad media las que se encuentren dentro del marco operacional o que se enmarquen en las medidas de protección.

Marco Organizativo

56 La medida 3.2 "Normativa de seguridad [org.2]": Priorizar las actuaciones precisas con el objeto de alcanzar la versión definitiva de la relación de normativa de seguridad identificada por el propio SAS. Esta circunstancia permitirá reforzar y, sobre todo, personalizar las prácticas de actuación que deben ser atendidas por el personal del SAS en el uso de los activos de información. **(Prioridad alta).**

57 La medida 3.3 "Procedimientos de seguridad [org.3]": Procedimientos de seguridad y el artículo 3.4 "Proceso de autorización [org.4]" proceso de Autorización: En la misma línea que la anterior recomendación, se debieran priorizar las actuaciones precisas con el objeto de 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).**

Marco Operacional

- *Medidas de seguridad: planificación*

58 La medida 4.1.2 "Arquitectura de seguridad [op.pl.2]": Dada la relevancia de la normativa relativa a la adquisición y aceptación de nuevos productos y servicios como factor crítico de éxito para el cumplimiento del Principio de Seguridad por Diseño, se considera necesario priorizar los esfuerzos con el objeto de alcanzar la versión definitiva no sólo de dicha normativa sino, de igual forma, de los distintos procedimientos que se deriven de la misma, y que permitan garantizar la efectividad del proceso en el contexto de los distintos activos de TI considerados en el alcance del ENS. **(Prioridad media).**

- *Medidas de seguridad: control de acceso*

59 La medida 4.2.1 "Identificación [op.acc.1]": 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 oportuno 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).**

60 La medida 4.2.2 "Requisitos de acceso [op.acc.2]": La formalización y aplicación de las guías y/o plantillas oportunas para la configuración de los distintos elementos TIC debiera venir acompañada de la elaboración de registro específico, a través del cual, se proceda a relacionar los distintos ficheros de configuración para cada recurso (activo de TI sobre el que se ha aplicado la guía o plantilla). **(Prioridad media)**.

61 La medida 4.2.7 "Acceso remoto [op.acc.7]": Acceso remoto: formalizar un procedimiento específico de actuación para la gestión de accesos remotos, aprovechando esta iniciativa para formalizar los periodos establecidos para las autorizaciones otorgadas. **(Prioridad media)**.

00287890

– *Medidas de seguridad: explotación*

62 La medida 4.3.1 "Inventario de activos [op.exp.1]": Inventario de activos: formalizar procedimientos específicos de actuación para el inventario de cada categoría de activos TIC de tal forma que, derivado de la normativa específica habilitada a tales efectos, se facilite la consecución del objetivo pretendido. **(Prioridad media)**.

63 La medida 4.3.2 "Configuración de seguridad [op.exp.2]": Configuración de seguridad: Elaboración de listas de chequeos específicas de verificación de configuraciones seguras con la información relativa a las funciones responsables de efectuar tales verificaciones, así como la fecha y versión de los procedimientos de fortificación utilizados. **(Prioridad media).**

64 La medida 4.3.4 "Mantenimiento [op.exp.4]": La formalización y aplicación del Plan de Mantenimiento específico exigido en dicha norma para las distintas categorías de activos, de tal forma que se puedan asociar planes de acción preventivo, predictivo y correctivos específicos ejecutados con periodicidad anual, con independencia de que el mantenimiento del activo de TI sea ejecutado internamente o se encuentre externalizado en terceros. **(Prioridad media).**

65 La medida 4.3.5 "Gestión de cambios [op.exp.5]": Priorizar los esfuerzos con el objeto de alcanzar la formalización de normativa y procedimiento de actuación específico para la gestión de cambios de tal forma que se pueda garantizar la identificación del ciclo de vida asociado a los cambios (análisis, decisión, niveles de autorización, priorización, pruebas previas a la ejecución, proceso de marcha atrás y monitorización posterior de los cambios), así como la formalización de registro de cambios en el contexto de los activos de TI afectados. **(Prioridad media).**

66 La medida 4.3.9 "Registro de la gestión de incidentes [op.exp.9]": Formalizar una instrucción específica con el detalle de las pautas de actuación que deben ser atendidas para garantizar la cadena de custodia de las evidencias, de tal forma que alineadas con las recomendaciones del CCN a tales efectos (CCN-STIC-817), se garantice la validez legal de tales evidencias relativas a incidentes. **(Prioridad media).**

– *Medidas de seguridad: servicios externos*

67 La medida 4.4.1 "Contratación y acuerdos de nivel de servicio [op.ext.1]": Formalizar las medidas de seguridad de NIVEL MEDIO que son de aplicación para el alcance de los contratos de prestación de servicios, atendiendo a la interpretación del Anexo I del ENS efectuado con carácter interno. No se corresponde lo expuesto en el Anexo VIII para el tratamiento de datos personales, con las expectativas planteadas para el análisis de riesgos de seguridad y la declaración de Aplicabilidad para el entorno de RECETA XXI. **(Prioridad media).**

68 La medida 4.4.2 "Gestión diaria [op.ext.2]": Formalización de una política específica para la formalización de los aspectos de seguridad que deberán ser considerados en la contratación y monitorización posterior (gestión diaria) de los servicios prestados por los proveedores (no sólo en el ámbito de la adquisición, desarrollo o mantenimiento de sistemas de información). **(Prioridad media).**

00287890

- *Medidas de seguridad: continuidad del servicio*

69 La medida 4.5.1 "Análisis de impacto [op.cont.1]": Formalización de metodología específica para la obtención de informe de Análisis de Impacto en el Negocio (BIA) como entrada de información precisa en el contexto del proceso de definición e implantación del Plan de Continuidad de Negocio para la infraestructura de TI del SAS. **(Prioridad media).**

Medidas de Protección

- *Medidas de seguridad: protección de infraestructuras e instalaciones*

70 La medida 5.1.1 "Áreas separadas y con control de acceso [mp.if.1]": No facilitar información sobre la ubicación del CIT en el contorno exterior del edificio al tratarse de áreas especialmente sensibles. **(Prioridad media).**

71 La **medida** 5.1.3 "Acondicionamiento de los locales [mp.if.3]": Proceder al desalojo de cualquier material inflamable (cartón, plástico, etc.) que pudiera encontrarse almacenado en el interior de los CPDs de Sevilla y Málaga. **(Prioridad media).**

- *Medidas de seguridad: gestión de personal*

72 La medida 5.2.1 "Caracterización del puesto de trabajo [mp.per.1]": Identificación de los requisitos específicos de seguridad para la posible identificación de necesidades formativas a incorporar en el Plan de Formación, siendo preciso un mayor desglose en detalle de los puestos de trabajo existentes en el SAS, ya que, según el grupo de colectivos (profesionales sanitarios, profesionales TIC, profesionales USTIC, …) los requisitos de formación y, sobre todo, de capacitación serán distintos. (Prioridad media).

- *Medidas de seguridad: protección de información*

73 La medida 5.7.4 "Firma electrónica [mp.info.4]": Alcanzar la formalización de una Política de Firma Electrónica del SAS aprobada por el órgano superior competente, así como un procedimiento específico con el detalle de las pautas de actuación que deben ser atendidas por los profesionales sanitarios en el uso de tales firmas electrónicas. **(Prioridad media).**

6.2. Recomendaciones sobre protección de datos

74 Se recomienda alcanzar la formalización del Modelo de Gobierno y Gestión de la Privacidad del SAS, a través del cual, puedan ser atendidas las siguientes consideraciones **(Prioridad alta):**

- La identificación de los objetivos que conforman la Estrategia de Privacidad del SAS mediante la formalización de la Política de Protección de Datos que, de igual forma, detalle la estructura de roles y responsabilidades para los procesos de toma de decisiones y ejecución de la operativa (por ejemplo, comités estratégicos y operativos debidamente representados), así como los niveles de monitorización y reporting precisos para comunicar a la dirección el grado de avance en la consecución de tales objetivos. Esta Política de Protección de Datos, desde el punto de vista práctica, debiera derivar en el cuerpo normativo de privacidad (estándares, procedimientos e instrucciones o guidelines de privacidad).

00287890

- El detalle del ciclo de vida operativo asociado a las distintas iniciativas de tratamiento a evaluar (garantías de Privacidad por Diseño), así como los distintos procesos de tratamiento de datos ya existentes e identificados en el Registro de Actividades de Tratamiento (RAT).
- Este ciclo de vida tendría en consideración desde el análisis oportuno para la evaluación de impacto, si procede, en el contexto de las nuevas iniciativas de tratamiento, o la documentación de la ficha de tratamiento asociada a los procesos ya existentes, hasta la identificación de los distintos riesgos de privacidad (incumplimiento de principios, derechos y obligaciones) a los que pudieran quedar expuestos tales tratamientos, y su estrategia de mitigación hasta alcanzar los niveles aceptables de riesgo formalizados por la Dirección (aplicación del Principio de Proporcionalidad en la adopción de medidas técnicas y organizativas para garantizar el cumplimiento). Las directrices de actuación consideradas por el SAS para la formalización de ciertos criterios demandados por el RGPD en determinados aspectos (determinación del nivel alto de riesgos, tratamiento de datos a gran escala, severidad de los impactos para su comunicación o no a los afectados, etc.) (adopción de actitud proactiva en la interpretación del marco normativo de aplicación en materia de protección de datos).

75 Formalizar un procedimiento especifico 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)**.

76 Con independencia de que tras el análisis oportuno se pudiera llegar a determinar que algunos de los derechos recogidos en los artículos 15 a 22 del RGPD no son de aplicación en el contexto de los procesos de tratamiento habilitados en el SAS, se considera oportuno reconsiderar el planteamiento de los criterios de actuación pertinentes frente al ejercicio de los siguientes derechos para el conocimiento por parte de los profesionales o unidades partícipes en la operativa de atención del ejercicio de derechos (derecho de supresión, derecho de limitación de la finalidad, derecho a la portabilidad de los datos, derecho de oposición, y derecho a no ser objeto de decisiones individuales automatizadas incluida la elaboración de perfiles) **(Prioridad media)**.

77 Formalización de procedimiento específico de actuación en el contexto de los procesos de selección de proveedores, de tal forma que, previa categorización del servicio a prestar en términos de sensibilidad y criticidad se haga efectiva la aplicación de mecanismos de garantías exigidas por la legislación de protección de datos **(Prioridad media)**.

78 A tenor de la anterior recomendación, se considera oportuna la formalización de procedimiento específico de actuación en el contexto de los procesos de monitorización de proveedores, de tal forma que, previa categorización del servicio a prestar en términos de sensibilidad y criticidad se haga efectiva la aplicación de mecanismos de garantías **(Prioridad media)**:

- La solicitud periódica de las certificaciones de seguridad y privacidad alcanzadas con relación a los servicios prestados.
- La aplicación de checklists de cumplimiento de principios, derechos y obligaciones elaborados al efecto según tipología de servicios prestados para su firma de conformidad por parte de los Encargados del Tratamiento, si procede, o la consideración de un Plan de Remediación en el caso de que se detectasen debilidades de cumplimiento.

00287890

- El mantenimiento de adhesión a algún código de conducta en materia de protección de datos y vinculado a los servicios que son prestados.
- El suministro de informe de auditoría con relación al cumplimiento de principios, derechos y obligaciones en el contexto de los servicios que serán prestados.

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

- Relación de Encargados del tratamiento principales (según categorización de servicios en términos de sensibilidad y criticidad) vinculados al proceso de tratamiento derivado de la prestación de servicios ejecutada.
- Relación de sistemas de información principales que actúan como soporte a la ejecución del proceso de tratamiento de datos.
- Referencia al análisis de riesgos de privacidad ejecutado en el contexto del proceso de tratamiento de datos, así como el Programa de Privacidad con el detalle de las medidas de privacidad (que no sólo de seguridad) que deben ser ejecutadas para la mitigación de los riesgos de incumplimiento de principios, derechos y obligaciones dentro de niveles aceptables.
- Referencia al análisis de Impacto de Privacidad (PIA) e informe de evaluación PIA, si procede asociado al proceso de tratamiento de datos.

80 Formalizar un procedimiento de mantenimiento del RAT, a través del cual, se concreten las siguientes pautas de actuación **(Prioridad media)**:

- Detalle de la información y de la documentación que debe acompañar a cada proceso de tratamiento de datos para su inclusión formal en el Registro de Actividades de Tratamiento.
- Secuencia lógica de actividades asociados a los procesos de alta, baja y modificación de procesos de tratamiento de datos.
- Detalle de las funciones y obligaciones del Responsable del Tratamiento (Dirección General) en términos de revisión y actualización periódica de la información/documentación asociada a los procesos de tratamiento de datos.

81 Incorporación de un anexo específico al procedimiento de gestión de incidentes de seguridad para la inclusión de los criterios de valoración de la magnitud de los riesgos en términos de privacidad, considerando las directrices emitidas por la Agencia Española de Protección de Datos a tales efectos **(Prioridad media)**.

00287890

7. APÉNDICE: INFORMACIÓN ADICIONAL

7.1. Metodología

A.1 La metodología de auditoría empleada ha mantenido 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 emitida por el CCN para la atención de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de Seguridad) del ENS.

A.2 La aplicación de esta metodología facilita la identificación de los riesgos existentes, ya provengan éstos derivados de deficiencias en la interpretación, diseño o concepción de las medidas de seguridad precisas, en el caso del ENS y de principios, derechos y obligaciones, en el caso de protección de datos (eficiencia asociada al proceso de evaluación y diseño de la estrategia de mitigación bajo un enfoque de gestión de riesgos de seguridad y aplicación del Principio de Proporcionalidad), o en la implantación y ejecución de tales medidas (efectividad de tales controles en términos de reducción del riesgo de privacidad).

A.3 Esta metodología, manteniendo como marco de referencia, los objetivos de control y cumplimiento legal establecidos en el ENS, ha tenido en cuenta las siguientes consideraciones:

- La evaluación de riesgos inherentes a las tecnologías de la información desplegadas, y a los procesos existentes para el procesamiento, almacenamiento o transmisión de la información en el ENS y a los procesos existentes para el tratamiento de los datos de carácter personal, en el caso de protección de datos.
- La ejecución de las pruebas necesarias para evidenciar si las medidas técnicas y organizativas demandadas según Declaración de Aplicabilidad y Anexo II del ENS y el cumplimiento de los Principios, Derechos y Obligaciones formalizados a través de la normativa vigente en materia de protección de datos, 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:

  - Entrevistas-testimonios obtenidos en el transcurso de las reuniones de trabajo planificadas.
  - Documentos formalmente emitidos en el contexto del cuerpo normativo de seguridad o en el ámbito de la protección de datos de carácter personal.

00287890

- Observaciones realizadas por el equipo auditor durante la auditoría in situ.
- Resultado de las pruebas específicas efectuadas por el equipo de auditoría en presencia de los auditados.

A.4 Para el establecimiento de los incumplimientos siguiendo lo establecido en la GPF-OCEX 4320 que se han identificado en la fiscalización del ENS y de protección de datos y sus efectos en el informe de fiscalización, se ha establecido la siguiente conversión, teniendo en cuenta lo establecido en la guía STIC-824 y CCN-STIC IC 01/19, donde:

- Incumplimiento leve o poco significativo: Los hallazgos identificados quedan categorizados como OBSERVACIONES.
- Incumplimiento significativo: Con independencia de los hallazgos identificados que quedan categorizados como OBSERVACIONES o NO CONFORMIDADES MENORES, se identifican NO CONFORMIDADES MAYORES, sin embargo, no se encuentran involucradas las medidas de seguridad que constituyen los procesos críticos de la guía CCN-STIC 824.
- Incumplimiento grave o muy significativo: Con independencia de los hallazgos identificados que quedan categorizados como OBSERVACIONES o NO CONFORMIDADES MENORES, se identifican NO CONFORMIDADES MAYORES encontrándose involucrada alguna de las medidas de seguridad que constituyen los procesos críticos.

7.2. Planes de auditoría

A.5 En el contexto del plan de auditoría se ha ejecutado el esquema de actividades que se detalla a continuación, siendo perfectamente válido para atender tanto el alcance, como los distintos objetivos formalizados para la auditoría del ENS y de Protección de Datos.

A.6 Este esquema es coherente y se encuentra alineado con las normas y directrices recogidas en el Marco Internacional para la Práctica Profesional de la Auditoría Interna emitidas por el IIA, los distintos estándares de control interno de TI detallados por ISACA, así como las pautas identificadas en la guía CCN-STIC 802 del CCN.

A.7 Como primera actividad, se mantuvieron las reuniones oportunas con el objeto de:

- Identificar las unidades organizativas afectadas, formalizando una primera relación de interlocutores válidos para el SAS.
- Planificar una agenda factible como calendario para la ejecución de la auditoría.

A.8 De igual forma, en esta etapa de planificación previa, se efectuó una primera solicitud de información / documentación precisa.

A.9 Esta información ha permitido alcanzar una contextualización y entendimiento del entorno técnico y funcional que debe ser auditado en términos de seguridad, así como el ajuste oportuno sobre el programa de auditoría.

A.10 El análisis de la documentación solicitada con carácter previo ha permitido:

- Identificar la categorización de los sistemas que actúan como soporte para la prestación del servicio de receta electrónica (RECETA XXI) y, con ello, la determinación de los niveles de

00287890

seguridad que podrán ser demandados en términos de autenticación de las partes, confidencialidad, integridad, disponibilidad y trazabilidad (dimensiones de seguridad consideradas en el contexto ENS).

- Evaluar inicialmente el modelo de Governance y la definición del marco de controles formalizado bajo un enfoque de riesgos de seguridad.

  En primera instancia, este entorno de control debe quedar formalizado a través de las directrices recogidas en las Políticas, Estándares y Normativas, así como las actividades de control o pautas de actuación identificadas en los procedimientos e instrucciones de seguridad correspondientes (cuerpo normativo de seguridad).

- Preparar el programa de auditoría para las jornadas de trabajo de campo in situ en las instalaciones del SAS según detalle de interlocutores alcanzado.

A.11 Como resultado del análisis de la documentación, y el detalle presentado en el cuerpo normativo de seguridad, se ha efectuado el diseño del programa de auditoría recogido en documento independiente y comentado internamente con los interlocutores oportunos del SAS.

A.12 Tal y como se ha indicado con anterioridad, el plan de pruebas ha precisado de diferentes técnicas de análisis focalizadas en entrevistas con los interlocutores oportunos, la observación de las instalaciones e infraestructuras de TI afectadas, o la planificación de pruebas técnicas específicas para la revisión de la infraestructura de controles implantada como estrategia de mitigación de los riesgos considerados en materia de seguridad de la información.

A.13 En cuanto al análisis y evaluación de resultados, se ha analizado de forma conjunta con los niveles de interlocución identificados por el SAS los resultados obtenidos tras la ejecución del Programa de Auditoría según alcance y objetivos anteriormente expuestos, con el objeto de lograr el consenso con relación a las conclusiones del trabajo de campo efectuado, y las debilidades de control identificadas.

A.14 Esta exposición ha permitido confirmar o matizar los escenarios y evidencias obtenidas con carácter previo a la identificación de las soluciones oportunas (acciones correctivas o complementarias de control).

A.15 Como etapa final de los servicios de auditoría, se emite el presente el Informe de Auditoría ENS.

7.2.1. Plan de auditoría del ENS

A.16 El programa de auditoría ha quedado conformado por las distintas medidas de seguridad que serán contrastadas en el contexto de los distintos activos de información que conforman la infraestructura tecnológica y de comunicaciones habilitada para los módulos de PRESCRIPCIÓN y DISPENSACIÓN en el entorno de información de RECETA XXI.

A.17 Estas medidas de seguridad han sido agrupadas según el siguiente detalle de dominios de seguridad manteniendo una relación directa con las 75 medidas de seguridad identificadas en el Anexo II del ENS, y sujetas a un análisis de aplicación según la Declaración de Aplicabilidad y la categorización alcanzada para el sistema en aplicación del Anexo I del ENS:

00287890

- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

  OBJETIVO DE CONTROL: Exposición de las funciones, obligaciones y responsabilidades de todas las partes afectadas en materia de seguridad de la información, con la designación formal de la figura del Responsable de Seguridad, y la identificación de los miembros que conforman el Comité de Seguridad de la Información que debiera encontrarse formalizado.

  La organización de la seguridad planteada debe alinearse con los principios de control interno asociados al modelo de aseguramiento y, por tanto, las funciones, obligaciones y responsabilidades de las partes interesadas debieran respetar el modelo de las tres líneas de defensa (dueño de los riesgos de la capa operativa, capa de monitorización y asesoramiento, y capa de auditoría interna o externa).

- GESTIÓN DE ACTIVOS DE INFORMACIÓN

  OBJETIVO DE CONTROL: Detalle de los criterios adoptados para la identificación e inventariado de los distintos activos de información existentes en la organización, con la designación formal del valor estratégico de seguridad establecido para cada activo TIC, y la identificación de su propietario.

  En el contexto de ejecución de esta actividad de análisis, por tanto, se debiera constatar la formalización del inventario actualizado de activos de información, así como las garantías demandadas en términos de autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.

  Por otro lado, se debiera analizar la formalización de un Estándar de Clasificación de los activos de información, de tal forma que quedan perfectamente expresadas las directrices de actuación para las siguientes actividades principales:

  - Los criterios de archivo y custodia de la información con independencia del soporte (electrónico o documental) en el que se encuentre.
  - Los criterios de distribución y publicación de la información.
  - Los criterios de intercambio de información con terceros.
  - Los criterios de procesamiento y almacenamiento de la información según determinados activos de TI (PC's, portátiles, pen drives, discos duros externos, tablets, smartphones, etc.).

- SEGURIDAD DEL PERSONAL

  OBJETIVO DE CONTROL: Pautas de actuación en materia de seguridad que deben ser consideradas para la ejecución de los procesos de selección y contratación de personal, así como frente a la terminación o extinción de la relación laboral, habiendo sido formalizado el procedimiento pertinente de asignación y restitución de activos de TI en los procesos de alta y baja de empleados, respectivamente.

  La redacción de estas prácticas de actuación debe permitir la sincronización de los tiempos de respuesta frente a las notificaciones de bajas de empleados, de tal forma que se pueda garantizar que la baja de un empleado provoca, indefectiblemente, y de forma inmediata, su imposibilidad de hacer uso de los recursos de TI con los que contaba anteriormente.

00287890

De igual forma, en este contexto de seguridad del personal, se tiene en consideración los aspectos referidos a la planificación de la formación, cualificación y concienciación del personal en materia de seguridad de la información, según el detalle de funciones, obligaciones y responsabilidades asignadas.

- SEGURIDAD FÍSICA Y AMBIENTAL

  OBJETIVO DE CONTROL: Detalle de las medidas de acondicionamiento adoptadas con relación a los Centros de Procesamiento de Datos habilitados, así como las medidas de seguridad y control establecidas en las distintas instalaciones para la prevención y/o detección de las situaciones de riesgo que puedan derivarse de desastres naturales (inundaciones, terremotos, etc.).

- CONTROL DE ACCESO LÓGICO A LOS SISTEMAS DE INFORMACIÓN

  OBJETIVO DE CONTROL: Consideración de las prácticas de actuación precisas para garantizar las dimensiones de seguridad relativas a la autenticidad, confidencialidad, integridad y trazabilidad de la información, contemplando las medidas de seguridad y controles específicos para la gestión de perfiles de acceso y cuentas de usuarios en sistemas de información y aplicaciones de negocio (procesos de alta y baja de usuarios), garantizando, con ello, la implantación de la oportuna política de mínimo privilegio.

  En el contexto del presente dominio, deben ser analizadas las actividades de monitorización precisas sobre los accesos efectuados desde el exterior (gestión de accesos remotos), y las condiciones de seguridad implementadas sobre los mismos, así como la relación de mecanismos de identificación y autenticación de usuarios implementados en función del valor estratégico de la información a la que se tendría acceso a través de tales mecanismos.

- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

  OBJETIVO DE CONTROL: Análisis de los procedimientos de actuación que, en materia de seguridad de la información, deben ser incorporados al ciclo de vida del desarrollo de software, ya sean estos ejecutados con carácter interno o mediante la prestación de servicios ofrecidos por terceras entidades de desarrollo.

  En este sentido, por tanto, quedarán identificados los controles de seguridad que deben ser implantados sobre las siguientes actividades:

  - Análisis de necesidades
  - Estudio de viabilidad
  - Detalle de escenarios
  - Especificación de requerimientos
  - Diseño
  - Construcción
  - Integración
  - Pruebas de validación
  - Despliegue o instalación
  - Mantenimiento

00287890

- GESTIÓN DE OPERACIONES, COMUNICACIONES Y REDES

  OBJETIVO DE CONTROL: En el contexto del presente dominio de seguridad, quedan englobados los procedimientos formalizados para la gestión de operaciones de sistemas (y, con carácter general, la infraestructura tecnológica y de comunicaciones), así como las pautas de actuación establecidas para garantizar la segregación de funciones, separación de entornos y clasificación de redes (criterios de interconexión de redes internas y externas).

  De igual forma, son considerados los procedimientos de actuación habilitados para la gestión de vulnerabilidades lógicas y la monitorización de los servicios de TI.

- GESTIÓN DE LA RELACIÓN CON PROVEEDORES

  OBJETIVO DE CONTROL: Análisis de los aspectos de seguridad que deben ser contemplados en la formalización de los procesos de selección y monitorización de proveedores (identificación previa de los requisitos de seguridad, elaboración de la matriz de valoración, definición de indicadores de nivel de servicio que puedan ser monitorizados durante la prestación del servicio, inclusión de cláusulas de confidencialidad y garantías de cumplimiento legal y continuidad en contratos de prestación de servicios, programas de monitorización y auditoría como mecanismos de garantía en la prestación del servicio, etc.).

- GESTIÓN DE INCIDENTES DE SEGURIDAD

  OBJETIVO DE CONTROL: En base al análisis funcional de servicios efectuado, así como de la infraestructura TIC de soporte habilitada, se analizará el modelo de gestión de incidentes de seguridad formalizado.

  Por tanto, se debe proceder a la revisión de los procesos planteados para la notificación, caracterización, escalado, gestión, respuesta, documentación y aprendizaje con relación a los incidentes de seguridad acaecidos sobre la infraestructura TIC, y con impacto sobre la ejecución de los procesos de negocio.

- GESTIÓN DE CONTINUIDAD DE NEGOCIO

  OBJETIVO DE CONTROL: En base al análisis BIA (Business Impact Analysis) y el análisis de riesgos de seguridad, se debiera formalizar la Estrategia de Continuidad de Negocio para los servicios considerados en el alcance según la categorización alcanzada por los mismos.

  En este contexto, por tanto, serían analizados los siguientes planes de actuación:

  - Plan de Activación
  - Plan de Emergencias
  - Plan de Comunicación
  - Plan de Actividades Transitorias
  - Plan de Recuperación frente a Desastres
  - Plan de Retorno

00287890

De igual forma, se analiza la determinación de la estructura organizativa necesaria para la posible activación de estos planes en el caso de que proceda (estructura organizativa crítica).

- CONFORMIDAD LEGAL

  OBJETIVO DE CONTROL: Análisis de las garantías ofrecidas con respecto a la identificación de requerimientos legales de aplicación según la actividad principal desarrollada por la organización, así como en los acuerdos establecidos con terceras partes interesadas (stakeholders).

  De igual forma, se analiza la planificación existente de revisiones o monitorizaciones periódicas internas y auditorías externas que son precisas en materia de seguridad de la información, ya sea en atención a requerimientos legales de obligado cumplimiento, o porque se consideren oportunas.

A.18 La revisión de estas medidas de seguridad para los distintos dominios identificados se ha efectuado en base a muestras representativas en términos de riesgos (materialidad).

A.19 Por otro lado, en aquellas situaciones en las que se ha considerado oportuno la revisión de parametrizaciones o configuraciones de seguridad en los sistemas de información, éstas han sido solicitadas al personal oportuno (administradores de sistemas y seguridad) evitando, tal y como se ha indicado con anterioridad, la posible ejecución de pruebas técnicas específicas sobre los sistemas directamente por parte del equipo de auditoría.

A.20 Por último, y con relación a los proveedores externos, con independencia del servicio prestado en el contexto de la seguridad de la información, ha sido analizado el contenido de los contratos de prestación de servicios con el objeto de evaluar las garantías ofrecidas, así como las actividades de monitorización interna del servicio prestado que se encuentran planificadas y ejecutadas.

7.2.2. Plan de auditoría de protección de datos

A.21 El Reglamento General de Protección de Datos, en su artículo 5.2, expone lo siguiente: "El Responsable del Tratamiento será responsable del cumplimiento de lo dispuesto en el artículo 5.1, y capaz de demostrarlo ("responsabilidad proactiva").

A.22 De igual forma, el RGPD, en su artículo 5.1 estipula que:

"Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia").
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines ("limitación de la finalidad").
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos").

00287890

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ("exactitud").
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales ("limitación del plazo de conservación").
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas ("integridad y confidencialidad")."

A.23 Este principio de responsabilidad proactiva, por tanto, no sólo determina la necesidad de atender los distintos principios fundamentales de protección de datos identificados en el artículo 5.1 de la norma RGPD, sino que, de igual forma, precisa la necesidad de poder evidenciar dicho cumplimiento.

A.24 Es, por ello, que el Programa de Auditoría RGPD elaborado ha quedado focalizado en la obtención de las evidencias oportunas relativas al cumplimiento de los Principios, Derechos y Obligaciones identificados por la normativa vigente en materia de protección de datos.

7.3. Cuadro Resumen Pruebas y Evidencias del ENS

MEDIDA	DIMENSIÓN*	CATEGORÍA**			Nº PRUEBAS	Nº EVIDENCIAS
ORG.01 – POLÍTICA DE SEGURIDAD	ACDIT	B	M	A	3	4
ORG.02 – NORMATIVA DE SEGURIDAD	ACDIT	B	M	A	5	5
ORG.03 – PROCEDIMIENTOS DE SEGURIDAD	ACDIT	B	M	A	5	3
ORG.04 – PROCESO DE AUTORIZACIÓN	ACDIT	B	M	A	3	2
OP.PL.01 – ANÁLISIS DE RIESGOS	ACDIT	B	M	A	2	3
OP.PL.02 – ARQUITECTURA DE SEGURIDAD	ACDIT	B	M	A	4	12
OP.PL.03 – ADQUISICIÓN DE NUEVOS COMPONENTES	ACDIT	B	M	A	1	2
OP.PL.04 – DIMENSIONAMIENTO / GESTIÓN DE CAPACIDADES	D		M	A	1	2
OP.PL.05 – COMPONENTES CERTIFICADOS	ACDIT			A	N/A	N/A
OP.ACC.01 – IDENTIFICACIÓN	AT	B	M	A	9	11
OP.ACC.02 – REQUISITOS DE ACCESO	ICAT	B	M	A	5	5
OP.ACC.03 – SEGREGACIÓN DE FUNCIONES Y TAREAS	ICAT		M	A	3	2
OP.ACC.04 – PROCESO DE GESTIÓN DE DERECHOS DE ACCESO	ICAT	B	M	A	2	1
OP.ACC.05 – MECANISMO DE AUTENTICACIÓN	ICAT	B	M	A	7	5
OP.ACC.06 – ACCESO LOCAL	ICAT	B	M	A	5	5
OP.ACC.07 – ACCESO REMOTO	ICAT	B	M	A	3	3
OP.EXP.01 – INVENTARIO DE ACTIVOS	ACDIT	B	M	A	2	2
OP.EXP.02 – CONFIGURACIÓN DE SEGURIDAD	ACDIT	B	M	A	4	4

00287890

MEDIDA	DIMENSIÓN*	CATEGORÍA**			Nº PRUEBAS	Nº EVIDECIAS
OP.EXP.03 – GESTIÓN DE LA CONFIGURACIÓN	ACDIT		M	A	2	3
OP.EXP.04 – MANTENIMIENTO	ACDIT	B	M	A	4	11
OP.EXP.05 – GESTIÓN DE CAMBIOS	ACDIT		M	A	5	3
OP.EXP.06 – PROTECCIÓN FRENTE A CÓDIGO DAÑINO	ACDIT	B	M	A	3	7
OP.EXP.07 – GESTIÓN DE INCIDENTES	ACDIT		M	A	2	2
OP.EXP.08 – REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS	T	B	M	A	3	2
OP.EXP.09 – REGISTRO DE LA GESTIÓN DE INCIDENTES	ACDIT		M	A	4	4
OP.EXP.10 – PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	T			A	N/A	N/A
OP.EXP.11 – PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS	ACDIT	B	M	A	2	1
OP.EXT.01 – CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO	ACDIT		M	A	2	13
OP.EXT.02 – GESTIÓN DIARIA	ACDIT		M	A	2	2
OP.EXT.03 – MEDIOS ALTERNATIVOS	D			A	N/A	N/A
OP.CONT.01 – ANÁLISIS DE IMPACTO	D		M	A	1	2
OP.CONT.02 – PLAN DE CONTINUIDAD	D			A	N/A	N/A
OP.CONT.03 – PRUEBAS PERIÓDICAS	D			A	N/A	N/A
OP.MON.01 – DETECCIÓN DE INTRUSIÓN	ACDIT		M	A	1	3
OP.MON.02 – SISTEMA DE MÉTRICAS	ACDIT	B	M	A	3	2
MP.INF.01 – ÁREAS SEPARADAS Y CONTROL DE ACCESO	ACDIT	B	M	A	2	7
MP.INF.02 – IDENTIFICACIÓN DE LAS PERSONAS	ACDIT	B	M	A	2	2
MP.INF.03 – ACONDICIONAMIENTO DE LOS LOCALES	ACDIT	B	M	A	4	4
MP.INF.04 – ENERGÍA ELÉCTRICA	D	B	M	A	4	6
MP.INF.05 – PROTECCIÓN FRENTE A INCENDIOS	D	B	M	A	1	3
MP.INF.06 – PROTECCIÓN FRENTE A INUNDACIONES	D		M	A	3	4
MP.IF.07 – REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO	ACDIT	B	M	A	1	1
MP.IF.08 – INSTALACIONES ALTERNATIVAS	D			A	N/A	N/A
MP.PER.01 – CARACTERIZACIÓN DEL PUESTO DE TRABAJO	ACDIT		M	A	2	5
MP.PER.02 – DEBERES Y OBLIGACIONES	ACDIT	B	M	A	3	9
MP.PER.03 – CONCIENCIACIÓN	ACDIT	B	M	A	2	4
MP.PER.04 – FORMACIÓN	ACDIT	B	M	A	3	5
MP.PER.05 – PERSONAL ALTERNATIVO	D			A	N/A	N/A
MP.EQ.01 – PUESTO DE TRABAJO DESPEJADO	ACDIT	B	M	A	2	N/A
MP.EQ.02 – BLOQUEO DE PUESTO DE TRABAJO	A		M	A	1	1
MP.EQ.03 – PROTECCIÓN DE EQUIPOS PORTÁTILES	ACDIT	B	M	A	3	5
MP.EQ.09 – MEDIOS ALTERNATIVOS	D			A	N/A	N/A
MP.COM.01 – PERÍMETRO SEGURO	ACDIT	B	M	A	1	3
MP.COM.02 – PROTECCIÓN DE LA CONFIDENCIALIDAD	C		M	A	2	3
MP.COM.03 – PROTECCIÓN DE LA AUTENTICIDAD E INTEGRIDAD	IA	B	M	A	4	6
MP.COM.04 – SEGREGACIÓN DE REDES	ACDIT			A	N/A	N/A
MP.COM.09 – MEDIOS ALTERNATIVOS	ACDIT			A	N/A	N/A
MP.SI.01 – ETIQUETADO	ACDIT	B	M	A	2	2

00287890

MEDIDA	DIMENSIÓN*	CATEGORÍA**			Nº PRUEBAS	Nº EVIDECIAS
MP.SI.02 – CRIPTOGRAFÍA	IC		M	A	1	1
MP.SI.03 – CUSTODIA	ACDIT	B	M	A	1	2
MP.SI.04 – TRANSPORTE	ACDIT	B	M	A	1	N/A
MP.SI.05 – BORRADO Y DESTRUCCIÓN	C	B	M	A	1	1
MP.SW.01 – DESARROLLO	ACDIT		M	A	3	6
MP.SW.02 – ACEPTACIÓN Y PUESTA EN SERVICIO	ACDIT	B	M	A	3	3
MP.INFO.01 – DATOS DE CARÁCTER PERSONAL	ACDIT	B	M	A	1	1
MP.INFO.02 – CALIFICACIÓN DE LA INFORMACIÓN	C	B	M	A	2	2
MP.INFO.03 – CIFRADO	C			A	N/A	N/A
MP.INFO.04 – FIRMA ELECTRÓNICA	AI	B	M	A	3	1
MP.INFO.05 – SELLOS DE TIEMPO	T			A	N/A	N/A
MP.INFO.06 – LIMPIEZA DE DOCUMENTOS	C	B	M	A	2	1
MP.INFO.09 – COPIAS DE SEGURIDAD (BACKUP)	D	B	M	A	4	6
MP.S.01 – PROTECCIÓN DEL CORREO ELECTRÓNICO	ACDIT	B	M	A	3	6
MP.S.02 – PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB	ACDIT	B	M	A	2	9
MP.S.03 – PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO	D		M	A	2	5
MP.S.04 – MEDIOS ALTERNATIVOS	D			A	N/A	N/A
				TOTAL	**169**	**240**

FUENTE: Elaboración propia. Cuadro nº 1
* A: autenticidad; C: confidencialidad; D: disponibilidad; I: integridad; T: trazabilidad
**B: básica; M: media; A: alta

7.4. Cuadro resumen medidas de seguridad del ENS

MARCO	MEDIDAS	MEDIDA DE SEGURIDAD	CONCLUSIÓN
MARCO ORGANIZATIVO	MARCO ORGANIZATIVO	ORG.1 POLÍTICA DE SEGURIDAD	CONFORME
		ORG.2 NORMATIVA DE SEGURIDAD	INCUMPLIMIENTO LEVE
		ORG.3 PROCEDIMIENTOS DE SEGURIDAD	INCUMPLIMIENTO LEVE
		ORG.4 PROCESO DE AUTORIZACIÓN	INCUMPLIMIENTO LEVE
MARCO OPERACIONAL	MEDIDAS DE SEGURIDAD: PLANIFICACIÓN	OP.PL.01 ANÁLISIS DE RIESGO	CONFORME
		OP.PL.02 ARQUITECTURA DE SEGURIDAD	CONFORME
		OP.PL.03 ADQUISICIÓN DE COMPONENTES	INCUMPLIMIENTO LEVE
		OP.PL.04 DIMENSIONAMIENTO DE CAPACIDAD	CONFORME
		OP.PL.05 COMPONENTES CERTIFICADOS	N/A
	MEDIDAS DE SEGURIDAD: CONTROL DE ACCESO	OP.ACC.01 - IDENTIFICACIÓN	INCUMPLIMIENTO SIGNIFICATIVO
			INCUMPLIMIENTO LEVE
		OP.ACC.02 – REQUISITOS DE ACCESO	INCUMPLIMIENTO LEVE
		OP.ACC.03 – SEGREGACIÓN DE FUNCIONES	CONFORME
		OP.ACC.04 – PROCESO DE GESTIÓN DE DERECHOS	CONFORME

00287890

		OP.ACC.05 – MECANISMOS DE AUTENTICACIÓN	INCUMPLIMIENTO SIGNIFICATIVO
		OP.ACC.06 – ACCESO LOCAL	INCUMPLIMIENTO SIGNIFICATIVO
		OP.ACC.07 – ACCESO REMOTO	INCUMPLIMIENTO LEVE
	MEDIDAS DE SEGURIDAD: EXPLOTACIÓN	OP.EXP.01 – INVENTARIO DE ACTIVOS	INCUMPLIMIENTO LEVE
		OP.EXP.02 – CONFIGURACIÓN DE SEGURIDAD	INCUMPLIMIENTO LEVE
		OP.EXP.03 - MANTENIMIENTO	CONFORME
		OP.EXP.04 – GESTIÓN DE LA CONFIGURACIÓN	INCUMPLIMIENTO LEVE
		OP.EXP.05 – GESTIÓN DE CAMBIOS	INCUMPLIMIENTO LEVE
		OP.EXP.06 – PROTECCIÓN FRENTE A MALWARE	CONFORME
		OP.EXP.07 – GESTIÓN DE INCIDENTES	CONFORME
		OP.EXP.08 – REGISTRO DE ACTIVIDAD DE USUARIOS	CONFORME
		OP.EXP.09 – REGISTRO DE GESTIÓN DE INCIDENTES	INCUMPLIMIENTO LEVE
		OP.EXP.10 – PROTECCIÓN DE LOS REGISTROS	N/A
		OP.EXP.11 – PROTECCIÓN DE CLAVES	CONFORME
	MEDIDAS DE SEGURIDAD: SERVICIOS EXTERNOS	OP.EXT.01 – CONTRATACIÓN Y SLAs	INCUMPLIMIENTO LEVE
		OP.EXT.02 – GESTIÓN DIARIA	INCUMPLIMIENTO LEVE
		OP.EXT.03 – MEDIOS ALTERNATIVOS	N/A
	MEDIDAS E SEGURIDAD: CONTINUIDAD DEL SERVICIO	OP.CONT.01 – ANÁLISIS DE IMPACTO	INCUMPLIMIENTO LEVE
		OP.CONT.02 – PLAN DE CONTINUIDAD DE NEGOCIO	N/A
		OP.CONT.03 – PRUEBAS PERIÓDICAS	N/A
	MEDIDAS DE SEGURIDAD: MONITORIZACIÓN DEL SISTEMA	OP.MON.01 – DETECCIÓN DE INTRUSIÓN	CONFORME
		OP.MON.02 – SISTEMA DE MÉTRICAS	INCUMPLIMIENTO SIGNIFICATIVO
MEDIDAS DE PROTECCIÓN	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE INFRAEST. E INSTALACIONES	MP.IF.01 – ÁREAS SEPARADAS Y CON CONTRO DE ACCESO	INCUMPLIMIENTO SIGNIFICATIVO
			INCUMPLIMIENTO LEVE
		MP.IF.02 – IDENTIFICACIÓN DE LAS PERSONAS	CONFORME
		MP.IF.03 – ACONDICIONAMIENT DE LOS LOCALES	INCUMPLIMIENTO LEVE
		MP.IF.04 – ENERGÍA ELÉCTRICA	CONFORME
		MP.IF.05 – PROTECCIÓN FRENTE A INCENDIOS	CONFORME
		MP.IF.06 – PROTECCIÓN FRENTE A INUNDACIONES	CONFORME
		MP.IF.07 – REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO	CONFORME
		MP.IF.09 – INSTALACIONES ALTERNATIVAS	N/A
	MEDIDAS DE SEGURIDAD: GESTIÓN DE PERSONAL	MP.PER.01 – CARACTERIZACIÓN DEL PUESTO DE TRABAJO	INCUMPLIMIENTO LEVE
		MP.PER.02 – DEBERES Y OBLIGACIONES	CONFORME
		MP.PER.03 – CONCIENCIACIÓN	CONFORME
		MP.PER.04 – FORMACIÓN	CONFORME
		MP.PER.05 – PERSONAL ALTERNATIVO	N/A
	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE EQUIPOS	MP.EQ.01 – PUESTO DE TRABAJO DESPEJADO	CONFORME
		MP.EQ.02 – BLOQUEO DE PUESTO DE TRABAJO	INCUMPLIMIENTO SIGNIFICATIVO
		MP.EQ.03 – PROTECCIÓN DE EQUIPOS PORTÁTILES	CONFORME
		MP.EQ.09 – MEDIOS ALTERNATIVOS	N/A
		MP.COM.01 – PERÍMETRO SEGURO	CONFORME

00287890

	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE COMUNICACIONES	MP.COM.02 – PROTECCIÓN DE LA CONFIDENCIALIDAD	CONFORME
		MP.COM.03 – PROTECCIÓN DE LA AUTENTICIDAD E INTEGRIDAD	CONFORME
		MP.COM.04 – SEGREGACIÓN DE REDES	N/A
		MP.COM.09 – MEDIOS ALTERNATIVOS	N/A
	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE SOPORTES	MP.SI.01 – ETIQUETADO	CONFORME
		MP.SI.02 – CRIPTOGRAFÍA	CONFORME
		MP.SI.03 – CUSTODIA	CONFORME
		MP.SI.04 – TRANSPORTE	CONFORME
		MP.SI.05 – BORRADO Y DESTRUCCIÓN	CONFORME
	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE APLICACIONES	MP.SW.01 – DESARROLLO	CONFORME
		MP.SW.02 – ACEPTACIÓN Y PUESTA EN SERVICIO	CONFORME
	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE INFORMACIÓN	MP.INFO.01 – DATOS DE CARÁCTER PERSONAL	N/A
		MP.INFO.02 – CALIFICACIÓN DE LA INFORMACIÓN	CONFORME
		MP.INFO.03 – CIFRADO	N/A
		MP.INFO.04 – FIRMA ELECTRÓNICA	INCUMPLIMIENTO LEVE
		MP.INFO.05 – SELLOS DE TIEMPO	N/A
		MP.INFO.06 – LIMPIEZA DE DOCUMENTOS	CONFORME
		MP.INFO.09 – COPIAS DE SEGURIDAD (BACKUP)	CONFORME
	MEDIDAS DE SEGURIDAD: PROTECCIÓN DE SERVICIOS	MP.S.01 – PROTECCIÓN DEL CORREO ELECTRÓNICO	CONFORME
		MP.S.02 – PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB	CONFORME
		MP.S.03 – PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO	CONFORME
		MP.S.04 – MEDIOS ALTERNATIVOS	N/A

FUENTE: Elaboración propia. **Cuadro nº 2**

7.5. Cuadro resumen incumplimientos de las medidas de seguridad del ENS

	Conformidad	Incumplimiento leve	Incumplimiento significativo	Incumplimiento muy significativo	N/A	TOTAL
MARCO ORGANIZATIVO						
MARCO ORGANIZATIVO	1	3	-	-	-	**4**
MARCO OPERACIONAL						
PLANIFICACIÓN	3	1	-	-	1	**5**
CONTROL DE ACCESO	2	3	3	-	-	**8**
EXPLOTACIÓN	5	5	-	-	1	**11**
SERVICIOS EXTERNOS	-	2	-	-	1	**3**
CONTINUIDAD DEL SERVICIO	-	1	-	-	2	**3**
MONITORIZACIÓN DEL SISTEMA	1	-	1	-	-	**2**
MEDIDAS DE PROTECCIÓN						
PROTECCIÓN DE INFRAEST. E INSTALACIONES	5	2	1	-	1	**9**
GESTIÓN DE PERSONAL	3	1	-	-	1	**5**
PROTECCIÓN DE EQUIPOS	2	-	1	-	1	**4**
PROTECCIÓN DE COMUNICACIONES	3	-	-	-	2	**5**
PROTECCIÓN DE SOPORTES	5	-	-	-	-	**5**
PROTECCIÓN DE APLICACIONES	2	-	-	-	-	**2**
PROTECCIÓN DE INFORMACIÓN	3	1	-	-	3	**7**
PROTECCIÓN DE SERVICIOS	3	-	-	-	1	**4**
TOTAL	**38**	**19**	**6**	**0**	**14**	**77***

***NOTA: Hay 2 medidas que llevan aparejadas dos conclusiones** **Cuadro nº 3**
FUENTE: Elaboración propia.

00287890

7.6. Cuadro resumen pruebas y evidencias del RGPD

	Nº PRUEBAS	Nº EVIDENCIAS
CUMPLIMIENTO DE PRINCIPIOS		
Principio de responsabilidad proactiva	1	6
Principio de licitud	1	2
Prinipio de transparencia	1	4
Principio de limitación de la finalidad	1	1
Principio de minimización	1	5
Principio de conservación	1	2
Principio de exactitud	1	2
Principio de integridad y confidencialidad	1	1
CUMPLIMIENTO DE DERECHOS		
Principio de cumplimiento de derechos	1	7
CUMPLIMIENTO DE OBLIGACIONES		
Privacidad por diseño	1	2
Relación con encargados	3	9
Registro de actividades de tratamiento	2	4
Análisis de riesgos de privacidad	2	2
Gestión de brechas de seguridad	1	2
Evaluación de impacto de privacidad	4	2
TOTAL	**22**	**51**

FUENTE: Elaboración propia. **Cuadro nº 4**

7.7. Cuadro resumen incumplimientos del RGPD

Capítulo	Apartado	Artículo	Consideración
II. Principios	Principios relativos al tratamiento	5.2	INCUMPLIMIENTO LEVE
IV. Responsable del tratamiento y encargado del tratamiento	Responsabilidad del responsable del tratamiento	24.1	INCUMPLIMIENTO LEVE
IV. Responsable del tratamiento y encargado del tratamiento	Responsabilidad del responsable del tratamiento	24.2	INCUMPLIMIENTO LEVE
IV. Responsable del tratamiento y encargado del tratamiento	Protección de datos desde el diseño y por defecto	25.1	INCUMPLIMIENTO LEVE
IV. Responsable del tratamiento y encargado del tratamiento	Evaluación de impacto relativa a la protección de datos	35	INCUMPLIMIENTO LEVE

FUENTE: Elaboración propia. **Cuadro nº 5**

00287890

8. ANEXOS

Anexo 8.1. Glosario de términos

ADMINISTRACIÓN ELECTRÓNICA	La utilización de las tecnologías de la información y la comunicación (TIC) en las administraciones públicas, asociada a cambios en la organización y nuevas aptitudes del personal. El objetivo es mejorar los servicios públicos, reforzar los procesos democráticos y apoyar a las políticas públicas.
ANÁLISIS DE IMPACTO DE PRIVACIDAD (PIA)	Se trata de una evaluación de impacto relacionada con la privacidad con el fin de identificar y analizar cómo la privacidad de los datos pueda verse afectada por determinadas acciones o actividades.
ANÁLISIS DE RIESGO	Utilización sistemática de la información disponible para identificar los peligros y estimar los riesgos.
ARQUITECTURA DE COMPONENTES	Se enfoca en la descomposición del diseño en componentes funcionales o lógicos que expongan interfaces de comunicación bien definidas. El objetivo es describir un sistema mostrando el diseño y el desarrollo del mismo.
AUTENTICACIÓN	Consiste en la verificación de las credenciales con las que se identificó el usuario, es decir, se demuestra que realmente es quién dice ser. Estas credenciales son conocidas como factores de autenticación.
AUTENTICIDAD	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
CATEGORÍA SISTEMA DE INFORMACIÓN	Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.
CIBERSEGURIDAD	Ver “seguridad de las redes y de la información”.
CONFIDENCIALIDAD	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información
CPD	Se denomina al edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y electrónico.
DIMENSIONES DE SEGURIDAD	A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas: Confidencialidad. Integridad. Trazabilidad. Autenticidad. Disponibilidad.
DISPONIBILIDAD	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
DOBLE FACTOR	El empleo de dos factores de autenticación de tipo distinto.
FACTORES DE AUTENTICACIÓN	Son aquellos mecanismos por los cuales se puede identificar un usuario. Generalmente, existen tres los factores que son: algo que el usuario sabe (ej. contraseña), algo que el usuario tiene (ej. código recibido por SMS) y algo inherente al usuario (ej. Huella dactilar).

00287890

GESTIÓN DE RIESGO	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
INTEGRIDAD (en relación con la seguridad de la información)	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
INTEGRIDAD (en relación con los controles de procesos/aplicación)	Completitud. (En las NIAs y otros documentos técnicos en inglés el término utilizado es "completeness", que se ha traducido como integridad, lo que puede inducir a confusión con su significado cuando se habla de seguridad de la información).
ISACA	Es el acrónimo de Information Systems Audit and Control Association, una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.
MEDIDAS DE SEGURIDAD	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción o de recuperación.
PRIVACIDAD DESDE DISEÑO	Se trata de un paradigma de gestión y desarrollo de proyectos que promueve la inclusión de la protección de la privacidad y los datos personales desde el inicio.
REGISTRO DE ACTIVIDADES DE TRATAMIENTO	Es una medida que obliga a las organizaciones a documentar los flujos de datos personales que circulan dentro de ellas.
SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN	Es la capacidad de las redes o de los sistemas de información de resistir, con un determinad nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. La ciberseguridad trata de la protección de los activos de información frene a las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.
SLA	Un acuerdo de nivel de servicio, también conocidas por las siglas SLA, es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)	Término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones.
TRAZABILIDAD	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Cuadro nº6

00287890

9. ALEGACIONES PRESENTADAS Y TRATAMIENTO DE LAS MISMAS EN EL SUPUESTO QUE NO HAYAN SIDO ADMITIDAS O SE ADMITAN PARCIALMENTE

ALEGACIÓN nº 1 al punto 54 (ADMITIDA)

00287890