Instrucción 8/2025, de 11 de abril, del director general del Servicio de Salud de las Islas Baleares por la que se aprueba el Código de buenas prácticas del Servicio de Salud en el uso de los sistemas de información, en el tratamiento de datos personales y en materia de inteligencia artificial

1. Los sistemas de información son elementos básicos para lograr los objetivos fundamentales encomendados al Servicio de Salud de las Islas Baleares, por lo que los usuarios deben usar estos recursos de manera que se preserven siempre las dimensiones de la seguridad sobre la información manejada y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

2. El uso de recursos tecnológicos para tratar la información tiene una finalidad doble para el Servicio de Salud:

   a) Facilitar y agilizar la asistencia sanitaria de atención primaria, de atención hospitalaria y de urgencia, así como tramitar los procedimientos administrativos usando herramientas informáticas y aplicaciones de gestión y garantizando el acceso a la información en tiempo real y la interoperabilidad entre los sistemas.

   b) Proporcionar información completa, homogénea, actualizada y fiable a los usuarios.

3. El uso del equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para desempeñar su actividad profesional, razón por la cual compete al Servicio de Salud determinar las normas, las condiciones y las responsabilidades bajo las que deben usarse tales recursos tecnológicos.

4. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril 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 (RGPD), determina que los datos deben ser tratados de tal

manera que se garantice una seguridad adecuada de estos, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, la destrucción o el daño accidental, aplicando medidas técnicas u organizativas apropiadas. Los responsables de tratamiento deben responsabilizarse de aplicar las medidas que garanticen un nivel de seguridad adecuado al riesgo. Ello implica ir adaptando las políticas de seguridad dependiendo de cómo evolucionen las amenazas en el ámbito de la protección de datos.

5. La Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), establece que los responsables de tratamiento han de determinar las medidas técnicas y organizativas apropiadas que deben aplicarse para garantizar y acreditar que se cumple el RGPD, la propia Ley, las normas que la desarrollan y la legislación sectorial aplicable.

6. Por su parte, 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, tiene por objeto establecer la política de seguridad en el uso de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, y establece los principios básicos y los requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

7. En el ámbito de la seguridad de la información es necesario tener en cuenta el Real decreto 43/2021, de 26 de enero, que tiene por objeto desarrollar el Real decreto ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y de los sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de los incidentes de seguridad.

8. Estos requerimientos se refuerzan con la obligación de garantizar una protección adecuada de los datos clínicos, derivada de aplicar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que establece diversas previsiones con la finalidad de proteger la confidencialidad y la intimidad relativas a la información relacionada con la salud de la ciudadanía.

9. En el ámbito autonómico, la Ley 5/2003, de 4 de abril, de salud de las Islas Baleares, establece los derechos y los deberes de la ciudadanía en el ámbito sanitario, entre ellos el derecho a la intimidad y a la confidencialidad de los datos que hagan referencia a la salud.

10. El Decreto 79/2023, de 22 de septiembre, por el que se establece la estructura orgánica básica del Servicio de Salud de las Islas Baleares, determina las funciones de la Subdirección de Transformación, Innovación y Salud Digital
—dependiente de la Dirección de Gestión y Presupuestos—, entre ellas establecer y promover la política de seguridad y los estándares mínimos y comunes relativos a la seguridad de la información de acuerdo con la normativa vigente en materia de protección de datos de carácter personal y la normativa específica en materia de seguridad de la información y ciberseguridad.

11. Por medio del Decreto 2/2018, de 23 de febrero, por el que se aprueba la política de seguridad de la información del Servicio de Salud de las Islas Baleares, dicho ente asume el mantenimiento de los niveles adecuados de seguridad y protección ante amenazas a la información que gestiona a partir de los objetivos establecidos en el artículo 5 del Decreto.

12. Toda esta normativa hace necesario incorporar al uso de las tecnologías de la información y de la comunicación las actuaciones que permitan garantizar un entorno seguro para el tratamiento adecuado de la información y que optimicen el uso de los recursos disponibles en la prestación de los servicios sanitarios.

13. En este sentido, con el objetivo de mantener unos niveles adecuados de protección de la información y de los recursos informáticos, el Servicio de Salud ha desarrollado las pautas necesarias para mantener las medidas de seguridad que garanticen que se cumple la normativa vigente y que se usan de manera adecuada y eficiente los recursos en la prestación de los servicios sanitarios. En efecto, cabe destacar lo siguiente:

    a) Por medio de la Circular 4/2009, de 28 de abril, del director general del Servicio de Salud, se aprobó el primer Código de buenas prácticas en el uso de los sistemas de información y el tratamiento de los datos de carácter personal del Servicio de Salud.

    b) De acuerdo con el Real decreto 311/2022 y con motivo de la necesaria gestión de los recursos tecnológicos de manera que proporcionen una protección adecuada de la información y de los

servicios, de la proliferación del uso de los dispositivos personales para fines profesionales, y de la aparición y la evolución de los servicios de almacenamiento en la nube, el director general del Servicio de Salud consideró oportuno aprobar la actualización del Código de buenas prácticas por medio de la Instrucción 4/2022, de 5 de mayo, que dejó sin efecto la Circular 1/2014, de 3 de marzo.

14. El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (IA) y por el que se modifican los reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828, regula la inteligencia artificial («AI Act») en la Unión Europea. Este Reglamento, que entró en vigor el 1 de agosto de 2024, tiene como objetivo principal fomentar una IA ética, fiable y centrada en el ser humano, que salvaguarde los derechos de los ciudadanos —asegurando que los modelos y sistemas de IA respetan la dignidad humana, la privacidad y la no discriminación— y que fomente la innovación permitiendo a las organizaciones desarrollar soluciones avanzadas en pro de la sociedad. Dicho Reglamento se basa en una clasificación de riesgos, en que las aplicaciones de IA se categorizan según su nivel de riesgo, para que se les apliquen los requisitos y las obligaciones proporcionales a su categoría.

15. Asimismo, en esta línea se han adoptado diversas guías e informes que abordan el uso ético y responsable de la IA en el ámbito de salud y se ha destacado la importancia de garantizar e implementar marcos de gobernanza robustos que incluyan la seguridad, la participación de todas las partes interesadas en la promoción de la transparencia, la rendición de cuentas y la protección de los derechos humanos. En este sentido, cabe destacar la guía de la Organización Mundial de la Salud *Ethics and governance of artificial intelligence for health*, que desarrolla este ámbito con la finalidad de guiar a las diversas organizaciones de salud pública y privada en la implementación de buenas prácticas y ética de la IA.

    Todo ello, en línea con la constante adaptación y actualización de las medidas adecuadas de mantenimiento de la seguridad de la información y protección de datos que lleva a cabo la Subdirección de Transformación, Innovación y Salud Digital, obliga a actualizar y aprobar una tercera versión del Código de buenas prácticas, que sustituye y deja sin efecto la versión anterior, aprobada por medio de la Instrucción 4/2022.

16. Este Código de buenas prácticas detalla las medidas —orientadas a los usuarios— que forman parte de la política de seguridad del Servicio de Salud, el cumplimiento de las cuales se considera imprescindible. Mantener los niveles adecuados de seguridad de la información depende en gran medida del hecho de que todos los usuarios apliquen estos criterios al desempeñar sus funciones y también de su compromiso, en primer lugar, de custodiar la información (especialmente los datos personales) contra el acceso, el uso o la divulgación no autorizados, la pérdida o la destrucción, y, en segundo lugar, de proteger los recursos informáticos utilizados para el tratamiento de esos datos del uso no autorizado, de la alteración, de la destrucción, del mal uso y del robo. Incorpora, además, la actualización y la adaptación a la nueva normativa aprobada en los ámbitos europeo y extraeuropeo relativa a la IA, teniendo en cuenta la trascendencia que supone y la constante evolución que experimenta, que obliga a adoptar medidas que garanticen la seguridad de la IA en un ámbito tan sensible como el de la salud.

Por todo ello, de conformidad con el artículo 12.1.*u)* del Decreto 39/2006, de 21 de abril, por el que se aprueban los estatutos del ente público Servicio de Salud de las Islas Baleares, el artículo 7.4 del Decreto 2/2018, de 23 de febrero, por el que se aprueba la política de seguridad de la información del Servicio de Salud de las Islas Baleares, y el artículo 21.2 de la Ley 3/2003, de 26 de marzo, de régimen jurídico de la Administración de la Comunidad Autónoma de las Islas Baleares, dicto la siguiente

Instrucción

1. Objeto

Esta instrucción tiene por objeto establecer las directrices y las recomendaciones en el tratamiento de los datos personales y en el uso de los sistemas de información a fin de optimizar el uso de los recursos disponibles y mantener la seguridad, la confidencialidad, la disponibilidad y la integridad de los datos personales, todo ello sin perjuicio de cumplir la normativa vigente.

2. Ámbito de aplicación

2.1. Todos los usuarios —tanto los empleados públicos como los adscritos a empresas externas públicas o privadas— que tengan acceso a los sistemas de información del Servicio de Salud de las

Islas Baleares y/o a los datos que figuren bajo la titularidad de este tienen que conocer y aplicar los requisitos y las instrucciones de este Código de buenas prácticas.

2.2. El Código es aplicable a todos los recursos —equipamiento físico, equipamiento lógico, servicios e información— usados por los usuarios para desempeñar sus funciones.

2.3. Es necesario garantizar la seguridad de la información a lo largo de todas las fases de su ciclo de vida (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y la de los sistemas que la soportan (análisis, diseño, desarrollo, implantación, explotación, integración y mantenimiento).

3. Definiciones

a) *Activo*: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (*software*), equipos (*hardware*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

b) *Archivo temporal*: archivo generado por un usuario durante el proceso de trabajo para almacenar información de forma provisional. Este tipo de archivo puede incluir documentos, imágenes, hojas de cálculo o cualquier otro tipo de archivo que se necesite durante una tarea específica.

c) *Autenticación*: procedimiento de comprobación de la identidad de un usuario.

d) *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.

e) *Autoridad de control*: autoridad pública independiente establecida por un estado miembro de la Unión Europea.

f) *Caracterización del puesto de trabajo*: definición de las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad y los requisitos que deben cumplir los usuarios en términos de confidencialidad.

g) *Centro de Atención a Usuarios (CAU)*: servicio que presta apoyo informático y gestiona las incidencias de los usuarios en relación con las aplicaciones y las infraestructuras informáticas.

h) *Confidencialidad*: propiedad o característica que consiste en no poner información a disposición de personas, entidades o procesos no autorizados ni revelársela.

i) *Consentimiento del interesado*: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, por medio de una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

j) *Correo basura*: también conocido como *spam*, es todo mensaje de correo electrónico no deseado que se envía aleatoriamente en procesos por lotes, al que está expuesta la mayoría de los usuarios. Es un modo extremadamente eficiente y barato de comercializar cualquier producto; de hecho, las encuestas confirman que más del 50 % de los mensajes de correo electrónico son correo basura. No es una amenaza directa, pero la cantidad de mensajes generados y el tiempo que lleva a las empresas y a los usuarios particulares detectarlo y eliminarlo supone una gran molestia.

k) *Dato anonimizado*: dato que no permite identificar a la persona afectada o interesada.

l) *Datos biométricos*: datos personales obtenidos a partir de un tratamiento técnico específico y que son relativos a las características físicas, fisiológicas o conductuales de una persona física y permiten o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

m) *Datos genéticos*: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, particularmente los obtenidos a partir del análisis de una muestra biológica.

n) *Datos personales*: toda información sobre una persona física identificada o identificable («el interesado»). Se considera *persona física identificable* toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular por medio de un identificador: un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

o) *Datos relativos a la salud*: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

p) *Delegado de protección de datos del Servicio de Salud*: persona física, jurídica u órgano que se encarga de garantizar que en la organización se cumplan las directrices del Reglamento (UE) 2016/679.

q) *Destinatario*: persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se consideran destinatarias las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión Europea o de sus estados miembros. El tratamiento de tales datos por dichas autoridades públicas ha de cumplir las normas en materia de protección de datos aplicables a los fines del tratamiento.

r) *Disponibilidad*: propiedad o característica de los activos que consiste en que las entidades o los procesos autorizados tienen acceso a aquellos cuando lo requieren.

s) *Elaboración de perfiles*: toda forma de tratamiento automatizado de datos personales que consista en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, a la situación económica, a la salud, a las preferencias personales, a sus intereses, a la fiabilidad, al comportamiento, o a la ubicación o los movimientos de dicha persona.

t) *Empresa*: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desarrollen regularmente una actividad económica.

u) *Encargado del tratamiento*: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

v) *Identificación*: procedimiento de reconocimiento de la identidad de un usuario.

w) *Incidencia*: cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

x) *Integridad*: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

y) *Inteligencia artificial*: sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que para objetivos explícitos o implícitos infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

z) *Limitación del tratamiento*: marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro.

aa) *Persona identificable*: toda persona cuya identidad pueda determinarse directa o indirectamente por medio de cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considera identificable si la identificación requiere plazos o actividades desproporcionados.

bb) *Programa malicioso*: código informático dañino que tiene como objetivo infiltrarse o dañar un equipo informático o sistema de información sin el consentimiento de su propietario.

cc) *Responsable de la seguridad*: responsable de determinar las decisiones para cumplir los requisitos de seguridad de la información y de los servicios en base a la declaración de aplicabilidad del Servicio de Salud. Actúa como punto de contacto con las autoridades competentes en materia de ciberseguridad y de supervisión de los requisitos de seguridad de las redes y los sistemas de información.

dd) *Responsable del tratamiento*: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y los medios del tratamiento. Si el derecho de la Unión Europea o de sus estados miembros determina los fines y los medios del tratamiento, el responsable del tratamiento o los criterios específicos para nombrarlo puede establecerlos el derecho de la Unión Europea o de sus estados miembros.

ee) *Riesgo*: posibilidad de materialización de una amenaza y consecuencias relativas a esa materialización.

ff) *Seudonimización*: tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que esta información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

gg) *Sistema de información*: conjunto de datos que interactúan entre sí con un fin común.

hh) *Teletrabajo*: trabajo que se realiza desde un lugar fuera de la empresa utilizando las redes de telecomunicación para cumplir las cargas laborales asignadas.

ii) *Tercero*: persona física o jurídica, autoridad pública, servicio u organismo distinto al interesado, al responsable del tratamiento, al encargado del tratamiento y a las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

jj) *Tratamiento de datos*: cualquier operación o conjunto de operaciones sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

kk) *Trazabilidad*: propiedad o característica que consiste en que las actuaciones de una entidad pueden imputarse exclusivamente a esta.

ll) *Usuarios*: todos los empleados públicos que prestan servicio en el Servicio de Salud y el personal de empresas externas que desarrolle tareas de manera permanente u ocasional en cualquier órgano perteneciente o adscrito al Servicio de Salud.

mm) *Violación de la seguridad de los datos personales*: toda violación de la seguridad que ocasione la destrucción, la pérdida o la alteración accidentales o ilícitas de datos personales transmitidos, conservados o tratados de otra forma, o bien la comunicación o el acceso no autorizados a dichos datos.

4. Información a los usuarios

4.1. Esta instrucción debe ponerse a disposición de todos los usuarios en la sede electrónica del Servicio de Salud. De la misma manera, debe enviarse a todos los usuarios un mensaje de correo electrónico que ha de contener los enlaces de consulta de la normativa.

4.2. En los manuales de bienvenida de las gerencias territoriales debe incorporarse el Código de buenas prácticas a fin de que las personas que se incorporen lo consulten antes de usar los recursos del Servicio de Salud.

4.3. Los órganos de dirección y de gestión del Servicio de Salud, estructurados en Servicios Centrales y en gerencias territoriales, son los responsables de hacer llegar esta norma a las empresas externas a fin de que sus usuarios la conozcan y la cumplan.

5. Confidencialidad de la información

5.1. Como medida de protección de la información propia, confiada o tratada por el Servicio de Salud, los usuarios deben abstenerse de comunicar dicha información, divulgarla, distribuirla o ponerla en conocimiento o al alcance de terceros (externos o internos no autorizados) por medio de soportes informáticos o por cualquier otro medio que no haya sido autorizado previamente.

5.2. Todo el personal del Servicio de Salud y el personal ajeno que, por razón de su actividad profesional, haya tenido acceso a información gestionada por el Servicio de Salud (datos personales, documentos, metodologías, claves, análisis, programas...) debe mantener una absoluta reserva sobre ella durante tiempo indefinido.

5.3. Si se tiene acceso en cualquier tipo de soporte a información que no sea de difusión libre, debe entenderse que el acceso es estrictamente temporal, mientras dure la función encomendada, que conlleva la obligación indefinida de secreto o de reserva y que ello no otorga derecho alguno de posesión, titularidad o copia de esa información. Asimismo, es imprescindible devolver los soportes de información usados inmediatamente después de que hayan terminado las tareas que hayan originado su uso.

5.4. Los usuarios solo pueden acceder a la información para la cual tengan la autorización debida y explícita dependiendo de las funciones que desempeñen, de tal manera que en ningún caso pueden tener acceso a información que pertenezca a otros usuarios o grupos de usuarios para el cual no tengan autorización.

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

5.5. Los derechos de acceso a la información y a los sistemas de información que la tratan deben otorgarse siempre de conformidad con los principios del mínimo privilegio posible y de la necesidad de conocer.

6. Protección de datos personales

6.1. Los usuarios con acceso a los datos personales o a los sistemas de tratamiento de datos están obligados a cumplir todas las medidas de seguridad establecidas y los requisitos y las condiciones aplicables de acuerdo con las normas y los procedimientos vigentes y los controles de seguridad establecidos. Así mismo, deben utilizar la información a la que tengan acceso solamente para los fines relacionados con sus competencias y exclusivamente para llevar a cabo el trabajo y desempeñar las funciones asignadas. Estos usuarios podrían tener que responder del hecho de incumplir estas obligaciones de conformidad con el régimen jurídico aplicable.

6.2. En las Islas Baleares, la protección de los datos personales está regulada por la normativa siguiente:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril 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 (RGPD).
- La Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), por la que se deroga la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

6.3. Basándose en la normativa vigente, se han desarrollado los criterios siguientes sobre las responsabilidades que debe asumir el responsable de tratamiento —o, en su caso, los representantes— del Servicio de Salud:

6.3.1. Tiene que designar un delegado de protección de datos para el Servicio de Salud.

6.3.2. Siempre que un tercero vaya a encargarse del tratamiento de los datos, debe ser bajo la relación jurídica de encargado del tratamiento.

6.3.3. Ha de mantener el registro de las actividades de tratamiento llevadas a cabo bajo su responsabilidad y hacer público un inventario de estas, accesible por medios electrónicos.

6.3.4. Debe tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de manera efectiva los principios básicos del RGPD y de la LOPDGDD.

6.3.5. Debe asegurarse de que se implanten correctamente las medidas de seguridad establecidas por el Esquema Nacional de Seguridad en el 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.

6.3.6. Tiene que adoptar medidas que garanticen que solo se tratarán los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

6.3.7. Ha de facilitar a los interesados el ejercicio de los derechos relativos a los datos personales, de manera que el procedimiento para ejercerlos sea visible, accesible y sencillo.

6.3.8. Debe notificar a la autoridad de protección de datos competente en un plazo máximo de 72 horas cuando se produzca un incidente de seguridad de los datos, a menos que sea improbable que la violación suponga un riesgo para los derechos y las libertades de los interesados.

6.3.9. Los datos solo pueden ser comunicados fuera del Espacio Económico Europeo si se cumplen los supuestos que se especifican en el procedimiento de transferencias internacionales de datos.

6.3.10. Ha de garantizar la formación y la capacitación necesarias en materia de protección de datos personales a las personas autorizadas para tratar datos personales.

6.3.11. Tiene que hacer consultas a la autoridad de control pertinente sobre los tratamientos de datos con el fin de garantizar que se cumpla la normativa de protección de datos vigente.

6.4. Sobre la base de la legislación establecida, se han desarrollado los criterios siguientes sobre las normas que deben cumplir todos los usuarios del Servicio de Salud con acceso a datos personales:

6.4.1. Es fundamental que los usuarios con acceso a datos personales guarden un estricto secreto profesional por tiempo indefinido sobre cualquier información a la que tengan acceso al desempeñar su trabajo. Ello implica que esta obligación sigue vigente incluso después de que se haya extinguido su relación con el Servicio de Salud.

6.4.2. Los usuarios tienen el compromiso de no tratar los datos personales a los que tengan acceso, ni cederlos, ni comunicarlos, ni utilizarlos en beneficio propio, ni revelarlos a terceros, y el compromiso de respetar siempre la privacidad y la confidencialidad de dichos datos.

6.4.3. Los usuarios deben conocer los principios básicos del RGPD y de la LOPDGDD requeridos para desempeñar las funciones que tiene asignadas. A continuación se detallan algunas consideraciones esenciales sobre dichos principios:

a) Todos los usuarios que tengan acceso a datos personales deben conocer la finalidad de usarlos y sus obligaciones particulares relativas al tratamiento requerido en el desempeño de su actividad profesional.

b) Los datos personales han de ser exactos y, si es necesario, actualizados; por ello deben adoptarse todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan.

c) El usuario que tenga acceso a datos personales debe extremar las precauciones para evitar la difusión o el acceso no autorizado y para no tratarlos sin la

autorización previa del responsable de tratamiento. Las cesiones de datos deben contar con habilitación legal y conforme a las medidas de seguridad aplicables, aunque es preferible —siempre que sea posible— comunicar solamente datos seudonimizados o anónimos.

d) Debe accederse a la información que contenga datos personales solamente por medio de los procedimientos habilitados a tal efecto por el Servicio de Salud.

e) Cualquier requerimiento nuevo para el tratamiento de datos personales que sea identificado —fuera de la actividad prevista— debe ser analizado y autorizado previamente por el delegado de protección de datos del Servicio de Salud.

f) Todos los usuarios deben colaborar para satisfacer el ejercicio de cualquiera de los derechos de acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento y no ser objeto de elaboración de perfiles, el ejercicio de los cuales se reconoce a los interesados, atendiéndoles correcta y adecuadamente e informándoles sobre cuál es el procedimiento que deben seguir.

g) Cualquier iniciativa, proyecto o desarrollo que vaya a iniciarse dentro del Servicio de Salud debe pasar por una fase de análisis de la privacidad desde el diseño y por defecto.

6.4.4. Quien tenga necesidad de generar archivos temporales debe asegurarse de los aspectos siguientes:

a) Ha de garantizar que el tratamiento cumple las finalidades autorizadas.

b) Ha de cumplir todas las medidas de seguridad establecidas de acuerdo con el nivel de riesgo identificado.

c) Ha de alojar los datos temporales en las unidades ofimáticas (carpetas) y en los sitios de Office 365 asignados a los usuarios por las unidades responsables en materia de tecnología de la información a fin de garantizar los controles técnicos

preestablecidos, y tiene que evitar alojarlos en un ordenador personal, siempre que sea posible.

d) Ha de eliminar o destruir convenientemente los archivos cuando dejen de ser necesarios para la finalidad para la que hayan sido creados.

6.4.5. Todo tratamiento que deba hacerse fuera de los sistemas de información del Servicio de Salud tiene que ser autorizado previamente y ha de cumplir las medidas necesarias para proteger la información.

6.4.6. Cuando se envíen por primera vez datos personales —en formato electrónico o impresos en papel—, hay que validar el método de envío a fin de garantizar que se cumplen las medidas de seguridad requeridas por el tratamiento.

6.4.7. De conformidad con el artículo 24 del Real decreto 311/2022, los sistemas de información que gestionen categorías especiales de datos personales deben generar un registro de accesos con la finalidad exclusiva de registrar las actividades de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas y permitir identificar en todo momento a la persona que actúa.

6.4.8. Los usuarios autorizados para gestionar soportes con datos de carácter personal deben guardarlos en un lugar seguro cuando no los usen, especialmente fuera de la jornada laboral. Adicionalmente, deben elaborar y mantener un inventario de los soportes que estén bajo su custodia. En caso de que se desechen o reutilicen los soportes, deben impedir que se pueda recuperar posteriormente la información almacenada.

6.4.9. Para tratar documentación que contenga datos personales es necesario observar las directrices siguientes:

a) A no ser que sea estrictamente necesario, hay que evitar imprimir en papel documentación que contenga datos personales.

b) Hay que poner un cuidado especial en no dejar documentos impresos con datos personales o confidenciales en la bandeja de salida de impresoras ni en los faxes, para evitar que estén al alcance de personas no autorizadas. De la misma manera, hay que evitar hacer fotocopias de dichos documentos; si se hacen, hay que controlar el uso que se les da y destruirlas oportunamente.

c) Los documentos deben guardarse en cajones o en armarios bajo llave en los periodos de ausencia del puesto de trabajo.

d) Las listas impresas que contengan datos con información personal no deben desecharse en los contenedores de papel para reciclar. Cada usuario debe revisar periódicamente los documentos que estén bajo su custodia y destruir los que sean obsoletos. La documentación impresa o en soporte óptico que contenga datos personales que tenga que desecharse debe eliminarse con máquinas destructoras de papel o mecanismos similares, o de alguna manera que evite que los datos se puedan recuperar.

6.4.10. Cualquier incidencia o anomalía que pueda afectar a la seguridad de los datos personales debe comunicarse al CAU o al servicio de informática correspondiente de acuerdo con el procedimiento de comunicación y gestión de incidencias.

7. Uso de los recursos informáticos

7.1. Pautas generales

7.1.1. El Servicio de Salud pone a disposición de los usuarios el acceso a determinados recursos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, que facilitan el desempeño de su trabajo. Estos recursos son propiedad del Servicio de Salud; como tales, deben utilizarse para las labores propias de los usuarios de acuerdo con las funciones asignadas. Con carácter general, los recursos informáticos y dispositivos de comunicaciones deben utilizarse para fines

institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

7.1.2. El Servicio de Salud es el responsable de determinar las normas, las condiciones y las responsabilidades oportunas para proteger los recursos informáticos. Los usuarios con acceso a estos son responsables de custodiarlos y de protegerlos ante las posibles amenazas (accesos no autorizados, uso indebido, errores u omisiones, robo, etc.).

7.1.3. Para no comprometer las medidas de seguridad establecidas por el Servicio de Salud, los usuarios deben evitar las acciones siguientes, salvo que dispongan de la autorización previa correspondiente:

a) Usar equipos o aplicaciones que no estén especificados directamente como parte del soporte lógico o del soporte físico estándar del Servicio de Salud. En ningún caso se puede modificar la configuración establecida de los recursos ni intercambiar componentes o periféricos (teclados, pantallas, ratones, etc.) entre ordenadores.

b) Extraer equipos de los locales o de las instalaciones del Servicio de Salud, salvo que esté autorizado previamente.

c) Hacer conexiones a redes o a sistemas externos o a la red corporativa por medios que no sean los definidos y administrados por el personal informático competente. En este sentido, hay que evitar especialmente establecer conexiones adicionales de manera independiente. También hay que evitar usar redes inalámbricas ajenas, pues pueden utilizarse para capturar información sensible o comprometer la seguridad de los sistemas que se conecten a ellas.

d) Extraer o utilizar información confidencial o datos personales en entornos que no estén protegidos o configurados adecuadamente para evitar el acceso no autorizado. Para exportar dichos datos a otros entornos hay que garantizar el nivel de seguridad correspondiente antes de extraerlos.

e) Trasladar fuera de las instalaciones habituales de trabajo datos o informaciones —en formato digital, impresos en papel o en cualquier otro soporte— sin la autorización previa correspondiente.

f) Destruir, alterar, inutilizar o dañar de cualquier otra manera los recursos informáticos, los programas, los datos, los soportes y los documentos.

g) Intentar descifrar las claves, los sistemas o los algoritmos de cifrado y cualquier otro elemento de seguridad establecido.

h) Modificar o desactivar los mecanismos de seguridad implantados para proteger los recursos informáticos y los sistemas de información.

i) Acceder a información que no sea necesaria para desempeñar las funciones de cada persona.

j) Dejar los recursos de tratamiento de información desatendidos sin las medidas de bloqueo adecuadas o mantener soportes con información sensible en lugares poco seguros.

k) Tener permisos de administrador de los equipos sin la autorización previa correspondiente.

7.1.4. El uso del ordenador, del dispositivo móvil, del navegador y del correo electrónico o de cualquier otro recurso para algún fin particular debe ser autorizado previamente.

7.1.5. Está prohibido expresamente utilizar los recursos informáticos para las finalidades siguientes:

a) Almacenar información con contenidos de carácter racista, xenófobo, pornográfico, sexual, de apología del terrorismo o que atente contra los derechos humanos, o que actúe en perjuicio de los derechos a la intimidad, al honor y a la imagen propia o contra la dignidad de las personas.

b) Instalar y/o usar programas o contenidos que atenten contra la legislación en materia de protección de la propiedad intelectual.

7.2. Uso de dispositivos móviles

7.2.1. Los dispositivos móviles —ordenadores portátiles, tabletas y teléfonos móviles— proporcionados por el Servicio de Salud deben disponer de las medidas de seguridad necesarias para garantizar su seguridad, las cuales deben basarse al menos en la instalación de sistemas de protección contra programas maliciosos y en actualizaciones y sistemas de protección de instalación de programas maliciosos.

7.2.2. Los dispositivos deben estar gestionados por los sistemas de gestión de dispositivos móviles del Servicio de Salud, que han de garantizar la seguridad de dichos dispositivos.

7.2.3. Los dispositivos móviles deben estar protegidos con contraseña y bloqueo automático por inactividad.

7.2.4. En ningún caso está permitido instalar aplicaciones no autorizadas por el Servicio de Salud o que puedan comprometer el funcionamiento de los dispositivos móviles.

7.2.5. Los dispositivos móviles del Servicio de Salud han de tener mecanismos de cifrado para impedir el acceso indebido de terceros no autorizados a la información que almacenen.

7.2.6. Los usuarios han de comunicar inmediatamente al CAU o al servicio de informática correspondiente la pérdida de su dispositivo móvil, a fin de que lo bloquee y borre su contenido.

7.2.7. Por motivos de seguridad, el Servicio de Salud puede bloquear los dispositivos móviles que presenten riesgos para la seguridad o pongan en peligro la confidencialidad de la información.

7.3. Uso de unidades ofimáticas

7.3.1. Con carácter general, la información almacenada de manera local en los ordenadores y equipos informáticos de los usuarios no será objeto de salvaguarda por medio

de ningún procedimiento corporativo de copia de seguridad. El Servicio de Salud puede hacer copias de seguridad de todos los activos y sistemas de información almacenados de manera local cuando disponga del conjunto de herramientas, medios y recursos para la generación de dichas copias.

7.3.2. El Servicio de Salud puede poner a disposición de los usuarios unidades ofimáticas y sitios de Office 365 —que consisten en espacio de disco en red asignado a cada usuario por el personal técnico del Servicio de Salud— para contener las salvaguardas periódicas de sus unidades locales. Tales unidades corporativas no deben utilizarse para fines privados, pues son una herramienta de trabajo, tienen una capacidad limitada y son compartidas por todos los usuarios, por lo que solo debe salvaguardarse la información que se considere estrictamente necesaria. En particular, hay que evitar almacenar en estas unidades —incluso con carácter provisional o temporal— contenidos de gran tamaño, como archivos multimedia (audio, vídeo, imágenes...).

7.4. Uso y mantenimiento de programas informáticos

7.4.1. Hay que evitar usar, instalar o distribuir programas fuera de las recomendaciones y de los estándares aprobados por el Servicio de Salud, ya que pueden comprometer la seguridad de los sistemas de información.

7.4.2. Si es necesario instalar programas ajenos al estándar establecido, hay que pedir autorización a la persona responsable del servicio, aunque es necesaria la valoración previa del servicio de informática correspondiente.

7.4.3. La instalación de programas informáticos debe ser siempre a cargo del servicio de informática correspondiente o debe ser monitorizada por este a fin de asegurar que se cumplen las medidas de seguridad requeridas y que se cuenta con las garantías de soporte oportunas. En ningún caso se pueden eliminar o deshabilitar las aplicaciones informáticas instaladas por

el servicio de informática, especialmente las relacionadas con la seguridad.

7.4.4. La instalación y el uso de programas debe hacerse de acuerdo con las licencias de uso adquiridas y controladas por el Servicio de Salud, por lo que está prohibido instalar programas sin la licencia correspondiente. Se prohíben la reproducción, la modificación, la transformación, la cesión, la comunicación y el uso fuera del ámbito del Servicio de Salud de las aplicaciones y de los programas informáticos instalados en los equipos que pertenecen a la organización. Tampoco está permitido hacer copias de los programas instalados en los ordenadores.

7.4.5. Los usuarios deben facilitar al CAU y al servicio de informática correspondiente el acceso a su equipo para labores de reparación, instalación o mantenimiento. Dicho acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que puedan encontrarse en el uso de los recursos informáticos y de comunicaciones, y terminará una vez que se haya completado el mantenimiento o se hayan resuelto los problemas.

7.4.6. Si el personal de soporte técnico detecta cualquier anomalía que indique que los recursos se utilizan de manera contraria a lo que establece este Código, informará de ello a la Subdirección de Transformación, Innovación y Salud Digital, que tomará las medidas correctoras oportunas.

7.4.7. Los equipos informáticos de la organización deben mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Hay que prestar especial atención a la actualización, la configuración y el funcionamiento correctos de los programas antivirus y cortafuegos.

7.5. Conexión de dispositivos personales

7.5.1. No se puede conectar en la red informática de comunicaciones corporativa (red interna) ningún

dispositivo distinto de los configurados, habilitados y admitidos por el Servicio de Salud, salvo que se disponga de la autorización previa correspondiente.

7.5.2. Los dispositivos personales usados en el ámbito del Servicio de Salud que accedan a las redes y aplicaciones corporativas pueden ser sometidos a actividades de prevención y control por el Servicio de Salud, aunque se limitarán a las áreas, las aplicaciones y los contenedores de información corporativa de los dispositivos personales en cuestión.

7.5.3. En caso de necesitar conectarse, el nivel de seguridad de los dispositivos personales debe ser el mismo que el de los dispositivos móviles corporativos empleados.

7.6. Sistemas de almacenamiento de información en la nube

7.6.1. El almacenamiento en la nube consiste en la disposición de aplicaciones, plataformas o infraestructura que, a cargo de un proveedor o del propio Servicio de Salud, están accesibles por medio de internet, independientemente de dónde estén alojados los sistemas de información, y de manera transparente para el usuario final.

7.6.2. Con carácter previo al uso de estos recursos externos, la Subdirección de Transformación, Innovación y Salud Digital debe establecer las características del servicio prestado y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de incumplirlo.

7.6.3. No está permitido transmitir o alojar información sensible, confidencial, datos personales o información protegida propia del Servicio de Salud en servidores externos o soluciones de almacenamiento en la nube distinta a las soluciones corporativas, salvo que se disponga de la autorización previa correspondiente. Debe comprobarse que no haya trabas legales para ello y verificar la suscripción de un contrato expreso entre el Servicio de Salud y la empresa responsable de la prestación del servicio, incluyendo los acuerdos de nivel

de servicio que sean procedentes, el correspondiente acuerdo de confidencialidad, y siempre habiendo analizado previamente los riesgos asociados.

7.7. Control de programas maliciosos

7.7.1. Un programa malicioso es un tipo de *software* que tiene como objetivo infiltrarse en un equipo informático o sistema de información o dañarlo sin el consentimiento de su propietario. La introducción de un programa malicioso en los sistemas de información del Servicio de Salud puede originarse al visitar páginas web infectadas, al abrir mensajes de correo electrónico o al ejecutar un programa contaminado o un archivo infectado (procedente de un disco duro externo, una memoria USB, un CD, un sistema de almacenamiento en la nube, un dispositivo móvil, etc.). El usuario debe ser consciente de las amenazas que ello provoca; por lo tanto, es imprescindible que haga un uso responsable de los equipos para reducir este riesgo.

7.7.2. Todos los puestos de trabajo y dispositivos móviles del Servicio de Salud deben tener instalados y activados los mecanismos adecuados para prevenir y detectar infecciones de programas maliciosos. En ninguna circunstancia deben desactivarse esos mecanismos; no obstante, hay que tener en cuenta que no garantizan la protección contra las amenazas, por lo que de manera general hay que actuar con cautela y sentido común:

a) Si se sospecha de una infección con un programa malicioso, virus, gusanos, *ransomware*, etc., hay que comunicar la incidencia de acuerdo con el procedimiento de comunicación y gestión de incidencias correspondiente.

b) Hay que adoptar todas las precauciones posibles al ejecutar cualquier programa, incluso los procedentes de fuentes consideradas de confianza, dado que pueden haber sido suplantados.

c) Hay que evitar ejecutar archivos adjuntos recibidos por correo electrónico y visitar páginas web con contenidos de legalidad o moralidad dudosas, pues son una fuente habitual de infecciones.

8. Medidas de seguridad

8.1. Medidas de seguridad de acceso físico

8.1.1. La información confidencial o con datos personales —en papel, en dispositivos de almacenamiento externo, en dispositivos móviles, en archivos visibles directamente en la pantalla del ordenador— debe custodiarse para evitar accesos no autorizados.

8.1.2. No debe mantenerse la información en sitios a la vista sin el control del responsable en ese momento. En caso de ausencia, es necesario establecer mecanismos que impidan el acceso de personas no autorizadas a esa información, de acuerdo con las características del puesto de trabajo y del soporte en el que esté la información.

8.1.3. Adicionalmente, las pantallas deben orientarse de tal manera que se elimine en la medida de lo posible el ángulo de visión a las personas no autorizadas.

8.2. Medidas de seguridad de acceso lógico

8.2.1. El control de acceso a los sistemas de información está basado en el uso de certificados electrónicos cualificados o identificadores de usuario y contraseñas ligadas a los perfiles de acceso. Dependiendo del nivel de seguridad de los sistemas, se requerirá un segundo factor de autenticación temporal. Estos perfiles han sido establecidos de acuerdo con las funciones que desempeña cada usuario y la criticidad de los sistemas.

8.2.2. El identificador de usuario y la contraseña correspondiente que se asignan al personal que los requiera son confidenciales, personales e intransferibles. Por tanto, es responsabilidad del titular el uso que se haga de ellos.

8.2.3. Cada usuario ha de velar por la confidencialidad de su sistema de segundo factor y la contraseña correspondiente; en ningún caso debe guardarla en

archivos digitales ni escrita en papel o en cualquier otro tipo de soporte de manera legible o accesible. Tampoco puede comunicar a otra persona su identificador de usuario ni su contraseña, ni debe usar una sesión abierta bajo otra identidad.

8.2.4. Si un usuario sospecha que su contraseña ha sido conocida de manera fortuita o fraudulenta por personas no autorizadas, debe modificarla y notificar inmediatamente la incidencia al servicio de apoyo correspondiente.

8.2.5. Cada usuario debe cambiar su contraseña de acceso a los sistemas al menos una vez cada tres meses y siempre que se lo indique el encargado de la gestión de usuarios.

8.2.6. Si, en un momento dado, un usuario recibe una llamada telefónica, un SMS o un mensaje de correo electrónico en el que se le solicita su nombre de usuario y/o su contraseña, nunca debe facilitar dichos datos y tiene que comunicar inmediatamente la incidencia al CAU o al servicio de informática correspondiente.

8.2.7. Cuando un usuario finalice su relación o vinculación con el Servicio de Salud, la persona directamente responsable del usuario debe comunicar esta nueva situación al encargado de la gestión de usuarios para que dé de baja las cuentas y las autorizaciones que tenga.

8.2.8. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por el Servicio de Salud estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tiene que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

8.3. Uso de certificados electrónicos como mecanismo de firma, identificación y autenticación

8.3.1. Todos los accesos a los sistemas que contengan información deben disponer de un mecanismo de identificación y autenticación que garantice la seguridad

de acceso al sistema. Este mecanismo está basado normalmente en el uso de identificadores de usuario y contraseñas, aunque en otros casos puede basarse en otros mecanismos que proporcionen un mayor grado de seguridad en base a la información que traten los sistemas de información.

8.3.2. El avance en la aplicación de los algoritmos criptográficos y en la certificación digital permite aplicar informáticamente procedimientos que tradicionalmente se han aplicado manualmente, con lo que se establecen garantías equivalentes respecto a la autenticación de la identidad de los actores y a la confidencialidad, la integridad y el no repudio de la información tratada.

8.3.3. El uso de esos algoritmos requiere que el usuario use un certificado electrónico, cuya autenticidad e integridad están garantizadas por un tercero de confianza. En este caso, el usuario debe observar las pautas siguientes:

a) En el uso del servicio, el usuario debe aplicar las prácticas establecidas por el Servicio de Salud y por la entidad prestadora de servicios de certificación que sean necesarias para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

b) El usuario debe comunicar cualquier variación de los datos aportados para obtener el certificado a la entidad prestadora de servicios de certificación y/o registro.

c) El usuario es el responsable del uso que se haga de su certificado electrónico.

d) El usuario debe salvaguardar el acceso a su certificado electrónico aplicando las medidas de seguridad descritas en el apartado 8.2 y ha de proteger cualquier elemento (tarjeta o dispositivo criptográfico, archivo informático, programa, PIN, contraseña, etc.) que sea necesario para acceder a esas claves. En ningún caso los dispositivos criptográficos que almacenen los certificados electrónicos deben quedar insertados en los lectores en ausencia del titular.

e) El usuario debe comunicar inmediatamente cualquier incidencia que afecte a la seguridad de su certificado electrónico o de los elementos y/o los códigos utilizados para acceder a este. Esta comunicación debe hacerse de acuerdo con los procedimientos establecidos por el Servicio de Seguridad de la Información.

8.4. Puesto de trabajo despejado

8.4.1. Con carácter general, los puestos de trabajo deben estar despejados, sin más material encima de la mesa que el que se requiera para la actividad que se haga en cada momento.

8.4.2. En particular, cuando un usuario del Servicio de Salud con acceso a los sistemas de información abandone su puesto de trabajo debe guardar toda la información que esté tratando, de manera que no queden desatendidos memorias USB o soportes externos de información, listas o información visible en la pantalla del ordenador personal o documentación sobre el propio puesto de trabajo. El material de trabajo debe guardarse en un lugar cerrado (en un cajón o un armario bajo llave) o en un cuarto separado cerrado con llave, al menos fuera del horario de trabajo.

8.4.3. Se puede establecer un procedimiento para revisar que se cumple esta medida haciendo una inspección regularmente después del cierre, notificando los incumplimientos detectados y retirando el material olvidado en un lugar cerrado.

8.5. Bloqueo del puesto de trabajo

8.5.1. Todos los terminales, ordenadores personales y dispositivos móviles usados por los usuarios del Servicio de Salud con acceso a la información en el desempeño de sus funciones deben ser bloqueados convenientemente por el usuario antes de abandonar su puesto de trabajo, tanto momentáneamente como al final de la jornada laboral.

8.5.2. Asimismo, debe bloquear el puesto de trabajo al cabo de un tiempo de inactividad, establecido por la política de seguridad, que es parte de la configuración del equipo y no puede ser alterado por el usuario.

9. Acceso por medio de redes

9.1. En el acceso y el uso de las redes implantadas en los diferentes centros del Servicio de Salud, todo usuario debe cumplir las normas de seguridad establecidas.

9.2. El acceso a las redes internas debe llevarse a cabo exclusivamente por los medios implantados corporativamente, por lo que no está permitido utilizar cualquier otro medio de conexión con redes externas sin la autorización previa correspondiente.

9.3. Para usar la red son necesarias las credenciales de acceso (generalmente un identificador, una contraseña y, en su caso, un segundo factor de autenticación), que se asignan solamente a los usuarios autorizados. La custodia de esas credenciales es responsabilidad del usuario autorizado, por lo que debe observar lo que disponen los apartados 8.2 y 8.3.

9.4. Cualquier conexión remota que se vaya a habilitar —a petición de un usuario interno o de un proveedor externo— debe tener la autorización previa de la persona responsable correspondiente y la validación de la Subdirección de Transformación, Innovación y Salud Digital a fin de garantizar los niveles de seguridad requeridos.

10. Uso de internet

10.1. Internet debe ser accesible a los usuarios que lo necesiten para desempeñar sus funciones, a quienes se proveerá de permisos de acceso.

10.2. En el uso de internet, el usuario debe ser consciente de que al desempeñar sus funciones laborales está representando al Servicio de Salud; consiguientemente, se compromete a reflejar en su conducta la ética, la profesionalidad, la cortesía y la responsabilidad que se espera de los usuarios que están adscritos a este organismo.

10.3. Debido a la necesidad de optimizar los recursos disponibles, el acceso a internet debe responder a fines profesionales. El Servicio de Salud velará por el buen uso del acceso a internet, tanto desde el punto de vista de la eficiencia y de la productividad de los usuarios como desde el punto de vista de los riesgos de seguridad asociados al uso de internet.

10.4. Sin perjuicio de lo que prevé el apartado 6.4.2 en relación con las cesiones, hay que evitar enviar datos personales por medio de internet. En cualquier caso, la transferencia solamente se puede efectuar usando los mecanismos que garanticen la ininteligibilidad y la integridad de los datos, y con la autorización previa correspondiente.

10.5. Es importante asegurar el cifrado en la transmisión de información sensible, confidencial o protegida. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar HTTP observando la barra de direcciones, en la cual también debería aparecer el icono de un candado, clicando en el cual se obtiene información sobre el certificado digital de identidad de la página web visitada.

10.6. No deben usarse navegadores ni programas de correo electrónico —ni versiones de estos— que no estén previstos por los estándares en vigor. Tampoco se puede modificar la configuración de esos programas en los aspectos relacionados con la seguridad.

10.7. Hay que notificar al CAU o al servicio de informática correspondiente cualquier anomalía detectada en el acceso a internet y toda sospecha de problemas o incidentes de seguridad relacionados con ese acceso.

10.8. Se consideran como uso incorrecto del servicio los casos siguientes:

10.8.1. Acceder a sitios de internet o distribuir mensajes con contenidos en que se incite o se promueva la pornografía o la segregación racial, sexual o religiosa, o con contenidos de violencia.

10.8.2. Descargar y transmitir indiscriminadamente imágenes, audios y vídeos, pues el tamaño de los archivos satura el

ancho de banda y disminuye la velocidad de transmisión, lo cual perjudica a los otros usuarios. Se prohíbe expresamente usar utilidades de intercambio de información en internet, como las redes de igual a igual (P2P, por *peer-to-peer*).

10.8.3. Distribuir virus o troyanos o llevar a cabo cualquier actividad a fin de acceder ilícitamente a otros sistemas de información con el objetivo de interceptar, dañar o manipular la información para obtener un beneficio personal, por diversión o para beneficiar o perjudicar a otras personas.

10.8.4. Llevar a cabo por medio de Internet cualquier actividad ilegal o maliciosa que ocasione molestias o daños a otras personas dentro o fuera del Servicio de Salud.

10.8.5. Hacer un uso inadecuado de cualquier material multimedia con derechos de la propiedad intelectual.

10.8.6. Utilizar el acceso a internet para el uso de servicios de mensajería instantánea no autorizados por el Servicio de Salud.

10.8.7. Almacenar información que contenga datos personales o confidenciales del Servicio de Salud en sistemas de almacenamiento, en dispositivos o en la nube que no dispongan de la validación de seguridad de la Subdirección de Transformación, Innovación y Salud Digital.

10.8.8. Transferir archivos no relativos a las actividades profesionales del usuario (juegos, archivos de audio, de imagen, de vídeo...).

10.8.9. Publicar en internet información relacionada con el Servicio de Salud, salvo que se disponga de la autorización previa correspondiente. En este sentido, los usuarios se comprometen a garantizar la privacidad de los datos y de las contraseñas de acceso y evitar difundirlos.

10.8.10. Llevar a cabo cualquier actividad de promoción de intereses personales.

10.9. Por motivos de seguridad y de rendimiento de la red del Servicio de Salud, el servicio de informática puede monitorizar y limitar el uso de internet. El sistema que proporciona el servicio de navegación puede disponer de filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva, servicios de redes sociales, servicio de almacenamiento en la nube, servicios de mensajería instantánea, servicios de videoconferencia no autorizados, aplicaciones no permitidas o páginas potencialmente inseguras o que contengan virus o programas maliciosos. Igualmente, el sistema puede registrar y dejar traza de las páginas a las que se haya accedido y del tiempo de acceso y del volumen y el tamaño de los archivos descargados. El sistema permite establecer controles que posibiliten detectar y notificar usos prolongados e indebidos del servicio.

11. Uso de herramientas de mensajería instantánea y sistemas de videoconferencia

11.1. El Servicio de Salud dotará al personal de herramientas de mensajería instantánea y sistemas de videoconferencias que cumplan los requerimientos legales vigentes.

11.2. En ningún caso se pueden utilizar servicios de mensajería instantánea o sistemas de videoconferencia no autorizados por el Servicio de Salud para comunicarse.

12. Uso del correo electrónico y de la agenda

12.1. El correo electrónico y la agenda proporcionados por el Servicio de Salud están destinados al uso profesional, pues son herramientas de trabajo. Es necesario tener la autorización previa correspondiente para cualquier uso particular, que debe ser puntual y limitado en frecuencia y duración. Dado que es un recurso compartido por todos los usuarios de la organización, un uso indebido repercute de manera directa en el servicio ofrecido a todos.

12.2. No se puede usar la dirección de correo electrónico del Servicio de Salud para registrarse en páginas web no institucionales y con fines particulares.

12.3. En ningún caso el uso autorizado para fines personales puede constituir una actividad comercial o con ánimo de lucro ni puede ser inapropiado u ofensivo. Se aconseja evitar también las actividades que exijan o aconsejen una privacidad especial, dadas las obligaciones del Servicio de Salud en cuanto a monitorización —según se desprende del apartado 16—, sin perjuicio del respeto estricto al derecho a la intimidad y al secreto de las comunicaciones.

12.4. El servicio de correo electrónico corporativo solamente debe usarse por los medios y las herramientas tecnológicas autorizados debidamente por el servicio de informática correspondiente.

12.5. Todo usuario autorizado para usar el correo electrónico y la agenda es responsable del uso que haga de ellos. Debe decirse que dispone de una capacidad de almacenamiento limitada, por lo que debe eliminar los mensajes que no sea necesario mantener almacenados.

12.6. El correo electrónico es un medio de comunicación interpersonal, no un medio de difusión masiva e indiscriminada de información. Debe evitarse toda práctica que pueda poner en riesgo el funcionamiento y el buen uso del sistema.

12.7. Está expresamente prohibido leer, borrar, copiar o modificar mensajes de correo electrónico o archivos dirigidos a otros usuarios, y revelar a terceros el contenido de cualquier dato reservado o confidencial que sea propiedad del Servicio de Salud o de terceros, salvo que tal actuación se lleve a cabo para cumplir fines estrictamente profesionales, con el consentimiento previo de los afectados.

12.8. Durante las tareas profesionales, en ningún caso deben enviarse comunicaciones desde cuentas de correo electrónico personales ofrecidas por proveedores de internet. Tampoco está permitido en ningún caso redirigir a cuentas particulares mensajes de correo electrónico de carácter profesional recibidos en la cuenta proporcionada por el Servicio de Salud.

12.9. Cuando se reenvíen correos electrónicos que hayan sido dirigidos a varios destinatarios, hay que evitar difundir las direcciones de correo electrónico de los destinatarios del mensaje original borrando esa información del mensaje reenviado, si es necesario.

12.10. Con carácter general, hay que evitar enviar información de carácter personal con datos de salud por medio del correo electrónico. Si es necesario hacer un envío de ese tipo, los datos deben estar cifrados.

12.11. Antes de abrir un mensaje de correo electrónico, hay que intentar detectar si se trata de un mensaje de procedencia dudosa o desconocida analizando su cabecera. En caso de duda, hay que borrar los mensajes sospechosos sin abrirlos o bien consultar al apoyo técnico.

12.12. Para evitar el correo masivo no solicitado (correo basura), como regla general solamente hay que facilitar la dirección de correo electrónico a personas conocidas. Cuando se reciban correos electrónicos desconocidos o no solicitados no hay que contestarlos, ya que al hacerlo se confirma la dirección.

12.13. Adicionalmente, se consideran como uso inadecuado del servicio de correo electrónico los casos siguientes:

12.13.1. Propagar contenido de carácter racista, xenófobo, pornográfico, sexual, de apología del terrorismo o que atente contra los derechos humanos, o que actúe en perjuicio de los derechos a la intimidad, el honor y la imagen propia o contra la dignidad de las personas.

12.13.2. Difundir mensajes de correo electrónico sin identificar plenamente al remitente. Si la cuenta de correo es usada por grupos de usuarios, hay que identificar al autor.

12.13.3. Divulgar mensajes comerciales o propagandísticos sin la autorización previa correspondiente.

12.13.4. Hacer circular cartas encadenadas y participar en esquemas piramidales o en actividades similares.

12.13.5. Utilizar el servicio con el objetivo de degradar el Servicio de Salud.

12.13.6. Enviar masivamente mensajes o información que consuman injustificadamente recursos tecnológicos.

12.13.7. Manipular la cabecera de los mensajes para intentar falsear u ocultar la identidad del remitente.

12.13.8. Instalar o emplear servidores o servicios de correo que no tengan la autorización previa correspondiente.

12.13.9. El sistema que proporciona el servicio de correo electrónico puede, de manera automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento del Código de buenas prácticas. Se puede insertar contenido adicional en los mensajes enviados para advertir a los receptores sobre los requisitos legales y de seguridad que deben cumplir con relación a dichos mensajes.

12.13.10. El uso de agendas telefónicas como herramienta de trabajo está sujeto al contenido y a los criterios de uso siguientes, ya que contienen información de carácter personal:

a) Los contenidos de las agendas corporativas solamente deben incluir la información siguiente: nombre y apellidos, función o puesto de trabajo, dirección postal o electrónica profesional, teléfono y número de fax profesionales.

b) El uso de las agendas debe ser exclusivamente el correspondiente a los contactos requeridos con el interesado y solamente para los fines solicitados por este.

13. Comunicación de incidencias de seguridad

13.1. El uso adecuado de los recursos informáticos evita que se produzcan incidentes que puedan ir en detrimento de la seguridad de la información, a la vez que garantiza un rendimiento óptimo. Por ello, cuando se detecten incidentes que puedan afectar a la seguridad de la información, es responsabilidad del Servicio de Salud llevar a cabo las actuaciones que se consideren convenientes y proporcionales para prevenir y/o corregir los riesgos identificados, por medio de la monitorización y el análisis de los recursos afectados para asegurar que se usan de la manera apropiada y para preservar la seguridad de los sistemas del Servicio de Salud.

13.2. Todo usuario que detecte un incidente que pueda tener un impacto significativo en la información manejada y en los servicios prestados debe comunicarlo inmediatamente al CAU, al servicio de informática correspondiente o al Servicio de Seguridad de la Información a fin de garantizar que el Servicio de Salud pueda cumplir las obligaciones en materia de protección de datos, seguridad de la información e infraestructuras críticas.

13.3. Todo usuario debe informar inmediatamente al CAU, al servicio de informática correspondiente o al Servicio de Seguridad de la Información sobre los incidentes que, a su juicio, puedan afectar a la seguridad de los activos del Servicio de Salud. En la notificación, el usuario debe indicar todos los detalles observados que le hayan hecho sospechar y ha de prestar la colaboración necesaria para resolver la incidencia. La obligación de informar es imprescindible para garantizar que se cumplan las obligaciones en materia de protección de datos, seguridad de la información, ciberseguridad e infraestructuras críticas.

13.4. Asimismo, los usuarios deben colaborar para mantener actualizadas las aplicaciones, pues es imprescindible que cooperen en la adaptación de los sistemas a los requisitos de cada momento. Para ello los usuarios deben comunicar por la vía oportuna cualquier deficiencia que observen o cualquier mejora que consideren adecuada.

13.5. Cuando una incidencia y/o deficiencia pueda causar un impacto grave en el funcionamiento del servicio sanitario, el usuario —de acuerdo siempre con el servicio de apoyo correspondiente— debe

adoptar las medidas de urgencia oportunas. Debe informar en detalle sobre los hechos acontecidos y las medidas adoptadas para que se registren y evalúen con la finalidad de aplicar las acciones necesarias.

14. Teletrabajo

14.1. En la modalidad de teletrabajo, el usuario debe aplicar todas las medidas aconsejadas descritas en los puntos precedentes y las que se describen en los siguientes.

14.2. Preferiblemente deben usarse los equipos de trabajo facilitados por el Servicio de Salud, que están equipados con las medidas de seguridad corporativas. Si el usuario solo puede usar su equipo personal, se aconseja que siga las pautas y recomendaciones de seguridad siguientes a fin de proteger adecuadamente la información y las comunicaciones:

- 14.2.1. Ha de crear contraseñas robustas y usar el doble factor de autenticación siempre que sea posible.
- 14.2.2. Debe mantener actualizados el sistema operativo y los programas instalados, tanto los de uso corporativo como los de nivel de usuario. Si se descarga otros programas, debe asegurarse que provienen de fuentes oficiales y que están autorizados.
- 14.2.3. Ha de disponer de un sistema antivirus actualizado periódicamente.
- 14.2.4. Debe cifrar los soportes de información a fin de proteger su contenido de posibles accesos malintencionados y, de esta manera, garantizar su confidencialidad e integridad.
- 14.2.5. Tiene que hacer copias de seguridad periódicamente.
- 14.2.6. Se denegará el acceso a cualquier dispositivo que no cumpla las medidas de seguridad mínimas.

14.3. En ningún caso el usuario puede trabajar con un equipo público que no sea el propio (p. ej., de un cibercafé, un hotel, un aeropuerto...).

14.4. Siempre que sea posible debe usar la red doméstica y evitar las redes wifi públicas. Si no es posible usar la red doméstica o, como alternativa, cualquier otra red que se considere segura, se recomienda que use la red de datos móviles propia.

14.5. Ha de acceder a la red interna y a los sistemas de información del Servicio de Salud usando exclusivamente los mecanismos corporativos habilitados, como las redes privadas virtuales (VPN) o los servicios corporativos de acceso remoto seguro.

14.6. Si tiene que participar en reuniones virtuales o hacer videollamadas, es aconsejable que use exclusivamente las herramientas corporativas habilitadas para tal efecto.

14.7. Durante la actividad profesional fuera de las instalaciones del Servicio de Salud el usuario ha de seguir las normas, los procedimientos y las recomendaciones internas vigentes.

14.8. El Servicio de Salud puede en cualquier momento limitar el acceso a sus redes y servicios publicados en internet a los equipos de los usuarios que no cumplan los requisitos mínimos de seguridad establecidos.

15. Uso de la IA

15.1. El Servicio de Salud promueve el uso responsable y seguro de la IA en su ámbito de actuación y debe garantizar que la implementación y el uso de la IA cumpla los principios de seguridad, ética, transparencia y respeto a los derechos fundamentales de los ciudadanos, de conformidad con la normativa vigente en materia de protección de datos y de gobernanza digital.

15.2. El desarrollo, el despliegue y el uso de sistemas de IA en el Servicio de Salud deben cumplir los principios siguientes:

15.2.1. Cualquier tratamiento de datos personales y todo sistema de IA deben ajustarse al RGPD, a la LOPDGDD y a la normativa de seguridad vigente. Hay que tener en cuenta especialmente que antes de implantar un sistema de IA es necesario hacer una evaluación del impacto que tendrá en la privacidad.

15.2.2. Queda estrictamente prohibido introducir, compartir o procesar datos confidenciales o datos de pacientes en sistemas de IA que no tengan la validación expresa del Servicio de Salud.

15.2.3. Todo sistema o algoritmo de IA que se prevea implantar en el Servicio de Salud debe contar con la autorización previa de los comités habilitados a tal efecto y de la validación expresa del Servicio de Salud. La supervisión del uso de dicho sistema o algoritmo ha de ser continua a fin de garantizar que cumple los estándares de seguridad, de calidad y de ética.

15.2.4. Los sistemas de IA tienen que operar de manera explicable y permitir la trazabilidad de las decisiones automatizadas. Los profesionales y los usuarios tienen que ser informados sobre el uso de la IA en los procesos en los que participen.

15.2.5. Deben establecerse medidas para evaluar y mitigar los riesgos asociados al uso de la IA, que han de incluir auditorías de seguridad, pruebas de robustez y sistemas de monitorización a fin de detectar posibles sesgos o usos indebidos.

15.2.6. Se permite utilizar la IA en los estudios de investigación sanitaria siempre que se cumplan los requisitos éticos, normativos y de protección de datos establecidos por el Servicio de Salud y los comités de ética pertinentes.

16. Finalización de la vinculación o relación con el Servicio de Salud

16.1. Cuando un usuario finaliza su relación o vinculación con el Servicio de Salud deja de tener acceso a los sistemas de información del Servicio de Salud y a los datos que contienen. Asimismo, tiene que devolver cualquier soporte que posea y que contenga datos a los que haya tenido acceso en el marco de su vinculación o relación con el Servicio de Salud.

16.2. También debe ceder el control sobre cualquier archivo o documento relativo a su prestación profesional; en caso de que haya creado archivos o documentos de carácter no profesional, debe eliminarlos.

17. Monitorización y aplicación del Código

17.1. Por motivos legales, de seguridad y de calidad del servicio, y a fin de cumplir en todo momento los requisitos que establece la legislación vigente, el Servicio de Salud ha de llevar a cabo las acciones siguientes:

17.1.1. Revisar periódicamente el estado de los equipos, los programas instalados, los dispositivos y las redes de comunicaciones que sean responsabilidad suya.

17.1.2. Monitorizar los accesos a la información que contengan sus sistemas.

17.1.3. Auditar la seguridad de las credenciales y de los programas.

17.1.4. Monitorizar los servicios de internet y de correo electrónico y otras herramientas de colaboración.

17.2. El Servicio de Salud ha de llevar a cabo esta actividad de monitorización sin utilizar sistemas o programas que puedan atentar contra los derechos constitucionales de los usuarios salvo en los supuestos en que sea estrictamente necesario con motivo de un requerimiento legal o una solicitud de colaboración de investigación.

17.3. Los sistemas en los que se detecte un uso inadecuado o que no cumplan los requisitos mínimos de seguridad pueden ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de la inseguridad o de la degradación haya desaparecido. La Subdirección de Transformación, Innovación y Salud Digital —con la colaboración de las restantes unidades del Servicio de Salud— velará por que se cumpla el Código de buenas prácticas e informará sobre los incumplimientos o las deficiencias de seguridad observados, a fin de que se tomen las medidas oportunas.

18. Cumplimiento del Código

18.1. Todos los usuarios del Servicio de Salud deben cumplir el Código de buenas prácticas.

18.2. Adicionalmente, los requisitos y las previsiones descritos en el Código se complementan con el resto de la normativa vigente y

con cualquier disposición legal de ámbito estatal o comunitario aplicable.

18.3. El incumplimiento de cualquiera de las pautas de comportamiento establecidas en el Código puede dar lugar a la responsabilidad disciplinaria correspondiente en aplicación de las normas reguladoras del régimen jurídico propio del usuario.

18.4. El uso de los recursos informáticos que el Servicio de Salud pone a disposición de los usuarios implica el conocimiento y la aceptación plena de las normas de uso, de las condiciones y de las advertencias legales que se especifican en el Código.

18.5. La Subdirección de Transformación, Innovación y Salud Digitalha de velar por que se cumpla el Código de buenas prácticas.

19. Difusión y publicación

19.1. Esta instrucción debe ser publicada en la sede electrónica del Servicio de Salud de las Islas Baleares y en los demás medios que este órgano de dirección considere oportunos.

19.2. El Servicio de Seguridad de la Información es el encargado de difundir esta instrucción.

20. Vigencia

Esta instrucción entra en vigor a partir de su publicación en la sede electrónica del Servicio de Salud y deja sin efecto la Instrucción 4/2022, de 5 de mayo, del director general del Servicio de Salud de las Islas Baleares por la que se aprueba el Código de buenas prácticas en el uso de los sistemas de información y el tratamiento de los datos personales.

El director general del Servicio de Salud