Código de buenas prácticas

Versión reducida

GOIB
CONSELLERIA
SALUT I CONSUM
SERVEI SALUT
ILLES BALEARS

Justificación

¿Por qué es necesario el Código de buenas prácticas?

- ✓ Los sistemas de información son básicos para conseguir los objetivos de la organización; por ello los usuarios deben usarlos preservando la seguridad.
- ✓ El uso de sistemas de información para tratar la información tiene una finalidad doble:
  - Facilitar y agilizar la asistencia sanitaria y tramitar los procedimientos administrativos.
  - Proporcionar información completa, homogénea, actualizada y fiable.
- ✓ El uso de equipamiento informático y de comunicaciones es una necesidad, por lo que se pone a disposición de los usuarios como instrumento de trabajo. Es competencia del Servicio de Salud determinar las normas, las condiciones y las responsabilidades para usarlo.
- ✓ También es un instrumento para cumplir la legislación vigente en materia de protección de datos, de seguridad de la información y sobre derechos y deberes de los ciudadanos.

¿Qué es un usuario?

Todo empleado público que preste servicio en el Servicio de Salud y el personal de empresas externas que desempeñe tareas de manera permanente u ocasional en cualquier órgano perteneciente o adscrito al Servicio de Salud.

¿Qué es un sistema de información?

Es un conjunto de datos que interactúan entre sí con un fin común.

Objeto y alcance

¿Cuál es el objeto del Código de buenas prácticas?

El objetivo es establecer las directrices y las recomendaciones que deben tener en cuenta todos los profesionales que trabajen para el Servicio de Salud sobre el uso de los sistemas de información, a fin de optimizar 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.

¿A quién debe aplicarse el Código de buenas prácticas?

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 o a los datos que figuren bajo su titularidad tienen que conocer y aplicar los requisitos y las instrucciones de este Código.

¿Sobre qué recursos debe aplicarse el Código de buenas prácticas?

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

¿Cuándo debe garantizarse la seguridad de la información? ¿Y la de los sistemas que permiten el tratamiento de la información?

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 en que se basa (análisis, diseño, desarrollo, implantación, explotación, integración y mantenimiento).

¿Qué es la disponibilidad?

Es la propiedad o característica que consiste en tener acceso a los datos o procesos cuando sean requeridos.

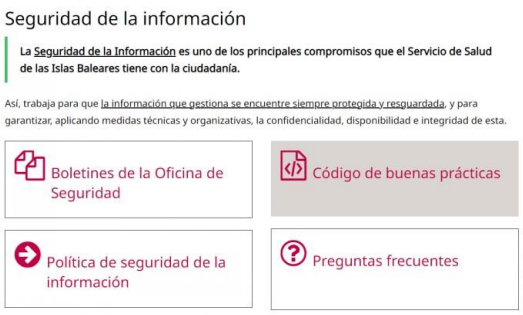
¿Qué es la integridad?

Es la propiedad o característica que consiste en que la información no ha sido alterada de manera no autorizada.

Información a los usuarios

¿Dónde se puede encontrar el Código de buenas prácticas?

- ✓ Está a disposición de todos los usuarios en el web del Servicio de Salud.
- ✓ Debe adjuntarse a los manuales de bienvenida de las gerencias territoriales, a fin de que los trabajadores que se incorporen lo consulten antes de usar los recursos del Servicio de Salud.



¿Quién debe encargarse de difundir esta norma?

Los órganos de dirección y de gestión del Servicio de Salud —estructurados en Servicios Centrales y en gerencias territoriales— son los responsables de difundir esta norma a las empresas externas, a fin de que sus usuarios la conozcan y la cumplan, así como el Servicio de Seguridad de la Información.

¿Qué ocurre si no se cumple el Código de buenas prácticas?

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.

¿Qué ocurre si se detecta un uso inadecuado de los sistemas o no se cumplen los requisitos mínimos de seguridad?

- ✓ Los sistemas pueden ser bloqueados o suspendidos temporalmente.
- ✓ El servicio se restablecerá cuando la causa de la inseguridad o de la degradación haya desaparecido.

Confidencialidad de la información

¿A qué se refiere la confidencialidad?

Es la propiedad o característica que consiste en no poner información a disposición de personas, entidades o procesos no autorizados ni revelársela.

¿Con quién se puede compartir la información a la que se tiene acceso por razones del trabajo?

- ✗ **Solo con el personal que tenga la autorización debida y explícita**. Como medida de protección de la información propia, confiada o tratada por el Servicio de Salud, los usuarios deben abstenerse de comunicarla, divulgarla, distribuirla o ponerla al alcance de otras personas (externas o internas no autorizadas) por medio de soportes informáticos o por cualquier otro medio que no se haya autorizado previamente.

¿Cuándo termina el compromiso de confidencialidad con el Servicio de Salud?

- ✗ **Nunca.** Todo el personal del Servicio de Salud y el personal ajeno que, por razón de la actividad profesional que desarrolle, haya tenido acceso a información gestionada por el Servicio de Salud (datos personales, documentos, metodologías, claves, análisis, programas, etc.) debe mantener una absoluta reserva durante tiempo indefinido, incluso después de que haya terminado su relación con el Servicio de Salud.

¿A qué información se puede acceder?

- ✓ Los usuarios solo pueden acceder a la información para la que tengan la autorización debida y explícita dependiendo de las funciones que desempeñen.
- ✓ 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.
- ✗ En ningún caso pueden tener acceso a información que pertenezca a otros usuarios o grupos de usuarios para la cual no tengan autorización.

¿En qué consisten los principios de *mínimo privilegio posible* y de *necesidad de conocer*?

En virtud de estos principios, los usuarios solo pueden acceder a la información y a los sistemas de información para los que tengan la autorización debida y explícita dependiendo de las funciones que desempeñen.

¿Qué debe hacer un usuario cuando termina su relación con el Servicio de Salud?

- ✓ Deja de tener acceso a los sistemas de información del Servicio de Salud y a los datos que contienen. Por ello tiene que devolver cualquier soporte que contenga datos a los que haya tenido acceso durante su relación con el Servicio de Salud.
- ✓ También debe ceder el control sobre cualquier archivo o documento relativo a su prestación profesional. Si ha creado archivos o documentos de carácter no profesional, debe eliminarlos.

Protección de datos de carácter personal

¿Qué es un dato de carácter personal?

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

¿Qué son los datos personales relativos a la salud?

Son datos personales relativos a la salud física o mental —incluida la prestación de servicios de atención sanitaria— que revelen información sobre el estado de salud.

¿Qué es el tratamiento de los datos?

Es cualquier operación o conjunto de operaciones sobre datos personales o conjuntos de datos personales, 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.

¿Qué medidas de seguridad hay que tener en cuenta para usar los sistemas de información y en el tratamiento de datos de carácter personal?

Como regla general, los profesionales deben seguir las pautas siguientes:

- ✓ Guardar estrictamente el secreto profesional por tiempo indefinido, incluso después de finalizada su relación con el Servicio de Salud.
- ✓ Conocer los principios del Reglamento general de protección de datos (Reglamento (UE) 2016/679) y la Ley orgánica 3/2018, de 5 de

diciembre, de protección de datos de carácter personal y garantía de los derechos digitales.

- ✗ Garantizar en cualquier caso la confidencialidad de los datos a los que tengan acceso (no enviar o compartir datos sin tener garantías sobre la identidad del destinatario). No acceder a los datos por medios distintos a los proporcionados por el Servicio de Salud.

¿Qué medidas de seguridad hay que aplicar para tratar la documentación impresa que contenga datos de carácter personal?

- ✗ Hay que evitar imprimir en papel documentación que contenga datos personales, si no es necesario.
- ✗ Hay que evitar que la documentación confidencial impresa quede al alcance de personas no autorizadas (en impresoras o fotocopiadoras, en el puesto de trabajo, etc.).
- ✓ Los documentos deben guardarse en cajones o en armarios cerrados con llave cuando se esté ausente del puesto de trabajo.
- ✓ Deben destruirse de manera segura (en contenedores reciclaje sellados o con máquinas destructoras de papel) los documentos confidenciales cuando se haya cumplido la finalidad para la que fueron generados.

¿Qué medidas de seguridad hay que aplicar si es necesario generar archivos temporales?

- ✗ Debe evitarse generar archivos temporales, pero si es estrictamente necesario deben eliminarse convenientemente cuando se haya cumplido la finalidad para la que fueron generados.
- ✓ Deben alojarse en las carpetas asignadas por la organización a fin de garantizar los controles técnicos establecidos.

¿Cuáles son las diferencias entre *interesado*, *responsable* del tratamiento y *encargado del tratamiento*?

El *interesado* (paciente) es la persona física titular de los datos cuya identidad pueda determinarse, directa o indirectamente, en particular por medio de un identificador (nombre, documento de identidad, datos de localización, identificador, etc.). El *responsable del tratamiento* es la persona física o jurídica, la autoridad pública, el servicio u otro organismo que, solo o con otros, determine los fines y los medios del tratamiento. El *encargado del tratamiento* es la persona física o jurídica, la autoridad pública, el servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

¿Qué es la figura de delegado de protección de datos y qué funciones tiene?

Es la persona física o jurídica o el órgano designado por el Servicio de Salud para que se encargue de garantizar que en la organización se cumplan las directrices del Reglamento general de protección de datos.

¿Qué es un dato anonimizado?

Es un dato que no permite identificar al interesado.

¿Qué es la seudonimización?

Es el tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que esta 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.

Uso de los recursos informáticos

¿Se pueden utilizar los recursos informáticos para uso personal?

- ✗ **Como norma general, no.** Solo deben utilizarse para las labores propias de los usuarios de acuerdo con las funciones asignadas.

¿Quién es el propietario de los recursos informáticos?

Son propiedad del Servicio de Salud, de manera que le corresponde determinar las condiciones y las responsabilidades para protegerlos y usarlos.

¿Cuáles son las responsabilidades de los usuarios?

Los usuarios son responsables de custodiar los recursos y de protegerlos de las posibles amenazas (accesos no autorizados, uso indebido, errores u omisiones, robo, etc.).

¿Cuáles son las prácticas que hay que evitar para no comprometer las medidas de seguridad establecidas por el Servicio de Salud?

- ✗ No deben usarse programas ni equipos informáticos que no sean los estándares del Servicio de Salud.
- ✗ No debe modificarse la configuración establecida.
- ✗ No deben sacarse equipos de los locales, excepto cuando esté autorizado previamente.

- ✗ No deben hacerse conexiones a redes o sistemas externos por otros medios que no sean los definidos y administrados por el personal competente.
- ✗ No deben extraerse o utilizarse información confidencial ni datos de carácter personal en entornos que no estén protegidos o configurados adecuadamente.
- ✗ No deben trasladarse fuera de las instalaciones habituales de trabajo datos o informaciones —impresos o en cualquier otro soporte, incluidos los digitales— sin la autorización previa correspondiente.
- ✗ No deben destruirse, alterarse o inutilizarse los recursos informáticos, los programas, los datos, los soportes ni los documentos.
- ✗ No debe intentarse descifrar las claves.
- ✗ No deben modificarse o desactivarse los mecanismos de seguridad implantados.
- ✗ No deben dejarse los recursos de tratamiento de información desatendidos sin las medidas de bloqueo adecuadas o mantener soportes con información sensible en lugares poco seguros.
- ✗ No debe accederse a la información que no sea necesaria para desempeñar las funciones propias.

¿Se pueden descargar música, películas y juegos en los equipos del Servicio de Salud?

No. Las unidades ofimáticas no deben utilizarse para fines privados, pues son una herramienta de trabajo con capacidad limitada y, además, se podría vulnerar la normativa en materia de protección de la propiedad intelectual.

¿Qué tipo de información se puede almacenar en las unidades ofimáticas?

Está prohibido expresamente almacenar información con 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, al honor y a la imagen propia o contra la dignidad de las personas.

¿Se pueden instalar programas en el equipo?

No, excepto con la autorización expresa del responsable del servicio y del servicio de informática.

¿Qué medidas de seguridad deben cumplir los dispositivos 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.
- ✓ Deben estar protegidos con contraseña y bloqueo automático por inactividad.
- ✓ Deben tener mecanismos de cifrado para impedir a las personas no autorizadas que accedan a la información que almacena n.

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

¿Cómo hay que actuar en un incidente de la seguridad con un dispositivo móvil?

- ✓ Si se pierde un dispositivo móvil, el usuario debe comunicarlo inmediatamente al Centro de Atención a Usuarios (CAU) o al servicio de informática correspondiente para que lo bloquee y borre el contenido.

¿Se pueden utilizar dispositivos personales para el trabajo?

- ✓ Los dispositivos personales utilizados en el ámbito del Servicio de Salud que accedan a las redes y aplicaciones corporativas pueden ser sometidos por el Servicio de Salud a acciones de prevención y control, aunque se limitarán a las áreas, las aplicaciones y los contenedores de información corporativa de esos dispositivos personales.
- ✗ Si es necesario que un dispositivo personal se conecte a las redes y aplicaciones corporativas, el nivel de seguridad del dispositivo ha de ser el mismo que el de los corporativos.
- ✗ No se puede conectar a 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.

¿En qué consiste el almacenamiento en la nube?

Consiste en la disposición de aplicaciones, plataformas o infraestructuras 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.

¿Se puede almacenar todo tipo de información en la nube?

- ✗ 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 distintas a las corporativas, salvo que se disponga de la autorización previa correspondiente.
- ✓ Debe comprobarse que no haya trabas legales para ello y verificar que se haya suscrito 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 acuerdo de confidencialidad correspondiente, y siempre habiendo analizado los riesgos asociados.
- ✓ Antes de usar estos recursos externos, la Subdirección de Tecnología de la Información 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.

¿Qué es un programa malicioso (*malware*)?

Es un tipo de *software* que tiene como objetivo infiltrarse en un equipo informático o sistema de información sin el consentimiento de su propietario.

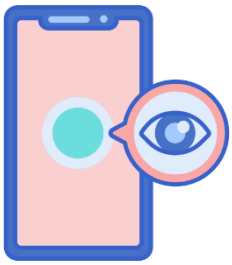
¿Qué medidas se pueden tomar para evitar los programas maliciosos?

- ✓ Si se sospecha que un equipo ha sido infectado por un programa malicioso, debe comunicarse la incidencia siguiendo el procedimiento correspondiente.
- ✓ Hay que adoptar todas las precauciones posibles al ejecutar cualquier programa, incluso aunque proceda de una fuente considerada de confianza, dado que puede haber sido suplantado por un programa malicioso.
- ✓ Hay que evitar ejecutar archivos adjuntos recibidos por correo electrónico y visitar páginas web con contenidos de legalidad o moralidad dudosas, pues habitualmente son una fuente de infecciones.

Medidas de seguridad

¿Cuáles son las medidas de seguridad principales de acceso físico?

- ✓ Los monitores de ordenador —especialmente los que estén en zonas con acceso del público— deben orientarse de tal manera que se elimine en la medida de lo posible el ángulo de visión a las personas no autorizadas.



- ✓ Debe custodiarse la información confidencial o con datos personales que figure en cualquier soporte digital o que sea visible directamente en el monitor del ordenador, a fin de evitar que se acceda a ella sin autorización.
- ✗ **No debe mantenerse información a la vista** sin el control del responsable en ese momento. Si está ausente, debe establecer los mecanismos oportunos según las características del puesto de trabajo y del soporte en el que esté la información para impedir que personas no autorizadas puedan acceder a ella.

¿Cuáles son las principales medidas de seguridad de acceso lógico?

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

- ✗ **Cada usuario ha de velar por la confidencialidad de su contraseña;** en ningún caso debe guardarla en archivos digitales ni escribirla en papel o en cualquier otro soporte que sea legible o accesible. Tampoco puede comunicar a otra persona su identificador de usuario ni su contraseña.
- ✗ En ninguna circunstancia puede utilizarse una sesión abierta con otra identidad.
- ✓ Si un usuario sospecha que su contraseña ha sido conocida de forma fortuita o fraudulenta por una persona no autorizada, debe modificarla y notificar inmediatamente la incidencia al CAU o al servicio de informática correspondiente.

- ✗ A la hora de crear una contraseña hay que procurar que otras personas no puedan adivinarla fácilmente.

- ✗ Todo usuario ha de cambiar la contraseña de acceso a los sistemas cada 45 días y siempre que lo indique el encargado de la gestión de los usuarios.
- ✗ Nunca debe facilitarse el nombre de usuario ni la contraseña si se piden por teléfono o correo electrónico. Además, debe comunicarse inmediatamente la incidencia al CAU o al servicio de informática correspondiente.
- ✓ Cuando un usuario finalice su relación o vinculación con el Servicio de Salud, su responsable directo debe comunicar la nueva situación al encargado de la gestión de los usuarios para que dé de baja las cuentas y las autorizaciones que tenga.

¿Se pueden utilizar otros mecanismos de identificación y autentificación?

- ✓ Sí, además del sistema basado en el uso de identificadores de usuario y contraseña se pueden utilizar algoritmos criptográficos y certificados digitales, con los cuales se establecen garantías equivalentes respecto a la autenticación de la identidad, a la confidencialidad, a la integridad y al no repudio de la información tratada.
- ✓ Se requiere que el usuario use un certificado electrónico, cuya autenticidad e integridad están garantizadas por un tercero de confianza.

El puesto de trabajo

¿Cómo debe mantenerse el puesto de trabajo?

Con carácter general, el puesto de trabajo debe mantenerse despejado, sin otro material sobre la mesa que el que se requiera para desarrollar la actividad de cada momento.

¿Qué hay que hacer cuando se abandona el puesto de trabajo?

- ✓ Hay que guardar toda la información que se esté tratando, de manera que no queden desatendidos memorias USB o soportes externos de información, listas o información visible en el monitor del ordenador o documentación sobre la mesa. Ese material debe guardarse en un cajón o un armario cerrado con llave o en un cuarto separado, igualmente cerrado, al menos fuera del horario de trabajo.
- ✓ Se puede establecer un procedimiento para revisar que se cumple esta medida haciendo regularmente una inspección después del cierre, notificando los incumplimientos detectados y retirando el material olvidado en un lugar cerrado.
- ✓ Es imprescindible bloquear los terminales y los dispositivos móviles con acceso a la información cuando no se esté trabajando con ellos, tanto momentáneamente como al final de la jornada laboral.

Acceso por medio de redes externas

¿Cuándo y cómo está permitido conectarse a las redes corporativas desde el exterior?

- ✓ Al acceder a las redes corporativas desde el exterior del Servicio de Salud, los usuarios deben cumplir las normas de seguridad establecidas.
- ✓ Debe accederse exclusivamente por los medios implantados corporativamente, de modo que no está permitido utilizar cualquier otro medio sin la autorización previa.

¿Se necesita autorización para habilitar conexiones remotas?

- ✓ Para usar las redes corporativas es necesario tener 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.
- ✓ Cualquier conexión remota que se vaya a habilitar —a petición de un usuario interno o de un proveedor externo— debe tener la autorización previa del responsable correspondiente

y la validación de la Subdirección de Tecnología de la Información a fin de garantizar los niveles de seguridad requeridos.

Uso de internet

¿Cuándo está permitido conectarse a internet?

- ✓ Internet debe ser accesible exclusivamente a los usuarios que lo necesiten para desempeñar las funciones asignadas.
- ✓ En el uso de internet, todo 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 trabajadores adscritos al Servicio de Salud.

¿Se pueden enviar datos personales por internet?

- × **No, debería evitarse.** En cualquier caso, solamente pueden enviarse usando los mecanismos que garanticen la ininteligibilidad y la integridad de los datos, y con la autorización previa correspondiente.

¿Cómo se puede asegurar la confidencialidad de la información que se transmitirá por internet?

Debe comprobarse en la barra de direcciones que se está utilizando el protocolo HTTPS (protocolo seguro de transferencia de hipertexto) en vez del protocolo estándar HTTP. En dicha barra 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.

¿A quién hay que notificar las anomalías detectadas en el acceso a internet?

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

¿Qué acciones se consideran como uso incorrecto de internet?

- × El acceso a sitios de internet y la distribución de mensajes con contenidos en que se incite o se promueva la pornografía y la segregación racial, sexual o religiosa, o con contenidos de violencia.
- × La descarga y la transmisión indiscriminada de imágenes o de archivos de audio o vídeo.
- × La distribución de virus o troyanos y cualquier actividad encaminada a acceder ilícitamente a otros sistemas de información.
- × 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.
- × Hacer un uso inadecuado de cualquier material multimedia con derechos de la propiedad intelectual.
- × Utilizar el acceso a internet para usar servicios de mensajería instantánea no autorizados por el Servicio de Salud.
- × 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 Tecnología de la Información.
- × Transferir archivos no relativos a las actividades profesionales del usuario (juegos, archivos de audio, de imagen, de vídeo, etc.).
- × La publicación en internet de información relacionada con el Servicio de Salud, salvo que se disponga de la autorización previa correspondiente.
- × Llevar a cabo cualquier actividad de promoción de intereses personales.

¿Se puede limitar el uso de internet?

- ✓ El sistema que proporciona el servicio de navegación puede disponer de filtros 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 y páginas potencialmente inseguras o que contengan virus o programas maliciosos.

- ✓ 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.

¿Qué es la trazabilidad?

Es la propiedad o característica que consiste en que las actuaciones de una entidad pueden imputarse exclusivamente a esta.

Herramientas de mensajería instantánea y sistemas de videoconferencia

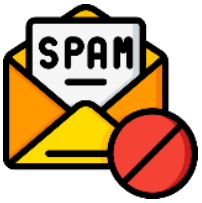
¿Se pueden usar herramientas de mensajería instantánea y sistemas de videoconferencia?

Sí. El Servicio de Salud dotará al personal de herramientas de mensajería instantánea y sistemas de videoconferencias que cumplan los requerimientos legales vigentes, pero solo los autorizados por el Servicio de Salud.

Correo electrónico y agendas corporativas

¿Qué es el correo basura?

Es todo mensaje de correo electrónico no deseado que se envía aleatoriamente en procesos por lotes, al que están expuestos la mayoría de los usuarios.



¿Qué se entiende por *correo electrónico profesional*?

El correo electrónico es una herramienta que proporciona el Servicio de Salud destinado al uso profesional; por lo tanto, es una herramienta de trabajo que necesita una autorización previa para cualquier uso particular, dado que es un recurso compartido por todos los usuarios de la organización, de modo que el uso indebido repercute directamente en el servicio ofrecido a todos.

¿Qué acciones se consideran como uso inadecuado del correo electrónico?

- × Utilizar la dirección de correo para registrarse en páginas web no institucionales y con fines particulares.
- × Utilizar el correo para actividades comerciales particulares o con ánimo de lucro.
- × Utilizar el correo para difundir mensajes inapropiados u ofensivos.
- × Es un medio de comunicación interpersonal, no un medio de difusión masiva e indiscriminada de información. Por ello debe evitarse toda práctica que pueda poner en riesgo el funcionamiento y el buen uso del sistema.
- × 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.
- × 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.
- × Divulgar mensajes comerciales o propagandísticos sin la autorización previa correspondiente.
- × Hacer circular cartas encadenadas y participar en esquemas piramidales o en actividades similares.
- × Utilizar el servicio con el objetivo de degradar el Servicio de Salud.
- × Enviar masivamente mensajes o información que consuman injustificadamente recursos tecnológicos.

- ✗ Instalar o usar servidores o servicios de correo que no tengan la autorización previa correspondiente.

¿Se pueden enviar datos de carácter personal por correo electrónico?

Con carácter general, hay que evitar enviar por correo electrónico información de carácter personal con datos de salud. Si es necesario enviarla, los datos deben estar cifrados.

¿Se puede acceder a los mensajes dirigidos a otros usuarios?

- ✗ **Está expresamente prohibido** leer, borrar, copiar o modificar mensajes de correo electrónico o archivos dirigidos a otros usuarios, y revelar a otras personas el contenido de cualquier dato reservado o confidencial que sea propiedad del Servicio de Salud o de terceros, salvo que deban cumplirse fines estrictamente profesionales, con el consentimiento previo de las personas afectadas.

¿Qué precauciones hay que tener para usar correctamente el correo electrónico?

- ✓ Solamente debe usarse por los medios y las herramientas tecnológicas autorizados debidamente por el servicio de informática correspondiente.
- ✓ Eliminar los mensajes que no sea necesario mantener almacenados, pues la capacidad de almacenamiento es limitada.
- ✓ Cuando se reenvíen mensajes de correo electrónico que hayan sido dirigidos a varios destinatarios, es conveniente no difundir las direcciones de los destinatarios del mensaje original borrando esa información antes de reenviarlo, a no ser que sea necesario conservarlas.
- ✓ Antes de abrir un mensaje de correo electrónico, hay que intentar averiguar si se trata de un mensaje de procedencia dudosa o desconocida. En caso de duda, hay que borrarlo sin abrirlo o consultar al CAU o al servicio de informática correspondiente.
- ✓ 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 mensajes de correo electrónico desconocidos o no solicitados no hay que contestarlos, pues al hacerlo se confirma la dirección.
- ✗ Durante las tareas profesionales, en ningún caso deben enviarse mensajes desde cuentas de correo electrónico personales.
- ✗ Tampoco está permitido en ningún caso redirigir a cuentas particulares mensajes de correo electrónico de carácter profesional recibidos en la cuenta corporativa del Servicio de Salud.

¿El sistema de correo electrónico puede de manera automatizada rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos?

- ✓ **Sí,** en los casos en que se detecte algún problema de seguridad o de incumplimiento del Código de buenas prácticas.
- ✓ Adicionalmente se puede insertar contenido adicional en los mensajes enviados para advertir a los receptores sobre los requisitos legales y de seguridad que deben cumplir en relación con dichos mensajes.

¿Cómo debe usarse la información de las agendas corporativas?

- ✓ El uso de las agendas debe ser exclusivamente el correspondiente a los contactos requeridos con el interesado y únicamente para los fines solicitados por este.
- ✗ En ningún caso deben utilizarse las direcciones incluidas en la agenda corporativa con fines particulares.

¿Se puede usar cualquier navegador o programa de correo electrónico?

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

¿Se puede usar el navegador o el correo electrónico para uso personal?

- ✗ **No.** Dada la necesidad de optimizar los recursos, 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.

Incidencias de seguridad

¿Qué es una incidencia?

Es cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

¿A quién deben notificarse las incidencias de seguridad?

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 ha de 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 importante para garantizar que se cumplan las directrices en materia de protección de datos, seguridad de la información, ciberseguridad e infraestructuras críticas.

¿Qué es el CAU?

Es el servicio que presta apoyo informático y gestiona las incidencias de los usuarios en relación con las aplicaciones y las infraestructuras informáticas.

¿Qué es un activo?

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

¿Qué hay que hacer si se detecta una deficiencia en una aplicación?

Dada la naturaleza dinámica y cambiante de los requisitos que han de satisfacer, los usuarios deben colaborar para mantener actualizadas las aplicaciones; por lo tanto, es imprescindible que cooperen en la adaptación de los sistemas a los requisitos de cada momento. Por ello deben comunicar por la vía oportuna cualquier deficiencia que observen o cualquier mejora que consideren adecuada.

Teletrabajo

¿Qué se entiende por *teletrabajo*?

Es el trabajo que se lleva a cabo desde un lugar fuera de la empresa usando las redes de telecomunicación.

¿Qué medidas deben aplicarse en la modalidad de teletrabajo?

- ✓ El usuario debe aplicar todas las medidas aconsejadas en el Código de buenas prácticas, como si se estuviese trabajando desde las instalaciones corporativas.
- ✓ Durante el teletrabajo, todo usuario ha de seguir las normas, los procedimientos y las recomendaciones internas vigentes.

¿Se puede utilizar un equipo personal para el teletrabajo?

Preferiblemente deben usarse equipos facilitados por el Servicio de Salud. Pero si solo se puede utilizar un equipo personal, hay que cumplir estas medidas de seguridad:

- ✓ Hay que crear contraseñas robustas y usar el doble factor de autenticación siempre que sea posible.
- ✓ Deben estar actualizados el sistema operativo y los programas instalados, tanto los de uso corporativo como los de nivel de usuario.
- ✓ Si se descargan otros programas, hay que asegurarse que provienen de fuentes oficiales y que están autorizados.
- ✓ Hay que disponer de un sistema antivirus actualizado periódicamente.
- ✓ Hay que cifrar los soportes de información a fin de proteger su contenido de accesos malintencionados.
- ✓ Hay que hacer copias de seguridad periódicamente.

¿Se puede utilizar un equipo público para el teletrabajo?

- ✗ **No.** En ningún caso se puede utilizar un equipo público que no sea el propio (p. ej., de un cibercafé, un hotel, un aeropuerto, etc.).

¿A qué redes es posible conectarse para el teletrabajo?

- ✗ Hay que evitar las redes wifi públicas.
- ✓ Siempre que sea posible debe usarse la red doméstica.
- ✓ Si no es posible usar la red doméstica o, como alternativa, cualquier otra red que se considere segura, se recomienda utilizar la red de datos móviles propia.

¿Cómo hay que conectarse con la red corporativa y otras partes del Servicio de Salud?

- ✓ Para acceder a la red interna y a los sistemas de información del Servicio de Salud hay que usar los mecanismos corporativos habilitados, como las redes privadas virtuales (VPN) o los servicios de acceso remoto seguro (Citrix, por ejemplo).
- ✓ Para participar en reuniones virtuales o hacer videollamadas, es aconsejable usar exclusivamente las herramientas corporativas habilitadas para tal necesidad.

¿El Servicio de Salud puede restringir el acceso a sus redes y a los servicios publicados en internet?

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