OTIC Seguretat

Govern de les Illes Balears
Servei de Salut

versión reducida

Código de buenas prácticas

OFICINA DE SEGURIDAD

Servicio de Salud de las Islas Baleares
Oficina de Tecnologías de la Información y Comunicación

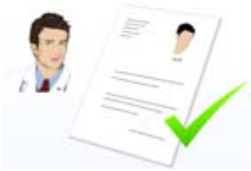
OBJETO Y ALCANCE

¿Cuál es el objeto del Código de buenas prácticas?

- El objeto del Código de buenas prácticas es definir los requisitos y las instrucciones que deben tener en cuenta todos los profesionales que trabajen para el Servicio de Salud en lo referente al uso de los recursos informáticos y el tratamiento de datos de carácter personal, a fin de mantener **su seguridad, confidencialidad, disponibilidad e integridad**.

¿Quién debe aplicar el Código de buenas prácticas?

- Todo el personal que tenga acceso a los sistemas de información del Servicio de Salud está obligado a conocer y aplicar los requisitos establecidos en el Código de buenas prácticas.



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

- Los requisitos establecidos por el Código de buenas prácticas se refieren al uso de todos los recursos (sistemas de información, ordenadores personales, medios de transmisión, etc.).

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

- Debe garantizarse durante la generación, la distribución, el almacenamiento, el procesamiento, el transporte, la consulta y la destrucción, además de la de los sistemas que la permiten (análisis, diseño, desarrollo, implantación, explotación, integración y mantenimiento).

¿Dónde puede encontrarse más información sobre el Código de buenas prácticas?

- La versión íntegra del Código de buenas prácticas está publicada en el web del Servicio de Salud (haga clic en este enlace): https://www.ibsalut.es/ibsalut/documentospdf/esp/CBP_SSIB_cast.pdf.

- Asimismo, desde el menú **Profesionales > Seguridad de la información** se puede acceder al curso interactivo sobre el Código de buenas prácticas.

CONFIDENCIALIDAD DE LA INFORMACIÓN

¿A qué se refiere la *confidencialidad*?

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

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

- **Nunca**. El personal que haya tenido acceso a datos de carácter personal al desempeñar su trabajo debe guardar estrictamente el secreto profesional durante tiempo indefinido, incluso después de que haya terminado su relación con el Servicio de Salud.

¿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 para la que 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 si no tienen autorización.

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

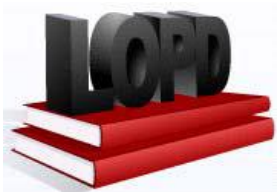
¿Qué es un dato de carácter personal?

Cualquier información numérica, alfabética, gráfica, fotografía, acústica o de cualquier otro tipo relativa a las personas físicas identificadas o identificables.

¿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.
- ✓ Conocer los principios de la Ley orgánica de protección de datos de carácter personal.
- ✓ Garantizar en cualquier caso la confidencialidad de los datos a los que tengan acceso.
- × No acceder a los datos por medios distintos a los proporcionados por el Servicio de Salud.



¿Qué medidas de seguridad hay que aplicar para el tratamiento de la documentación impresa en papel que contenga datos de carácter personal?

- ✓ Guardar la documentación confidencial en cajones o armarios cerrados con llave.
- ✓ Destruir de manera segura la documentación confidencial.
- × Evitar generar documentación impresa.
- × Evitar que la documentación confidencial impresa en papel quede al alcance de personas no autorizadas (en impresoras, faxes, puestos de trabajo...).
- × Evitar generar archivos temporales.
- × Evitar dejar información confidencial desatendida (memoria USB sin cifrar o sin guardar, equipos sin bloquear...).

¿Qué es un dato personal relativo a la salud?

En particular, se consideran datos relativos a la salud los referidos al porcentaje de discapacidad y a la información genética.

USO DE LOS RECURSOS

¿Se pueden utilizar los recursos informáticos para uso personal?

- **Como norma general, no.** Solo deben usarse para las labores propias del personal de acuerdo con las funciones que tiene asignadas.

¿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 ningún dato ni información alguna sin la autorización 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 debe accederse a la información que no sea necesaria para desempeñar las funciones de cada trabajador.

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

- No. Las unidades ofimáticas no deben utilizarse para fines privados, ya que constituyen una herramienta de trabajo y tienen capacidad limitada.

¿Se pueden instalar programas en el equipo?

- No, excepto con la autorización expresa del responsable del servicio y del Servicio de Informática.

¿Qué es un sistema de información?

Es un conjunto de ficheros —automatizados o no—, programas, soportes y equipos usados para almacenar y tratar los datos.

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

- **No.** Con carácter general está prohibido transmitir o alojar información sensible, confidencial, datos de carácter personal o información protegida propia del Servicio de Salud, salvo que previamente se disponga de la autorización 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.

- ✓ Antes de utilizar estos recursos externos, la Subdirección de la OTIC debe establecer las características del servicio prestado y las responsabilidades de las partes.

¿Qué es un código maligno?

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

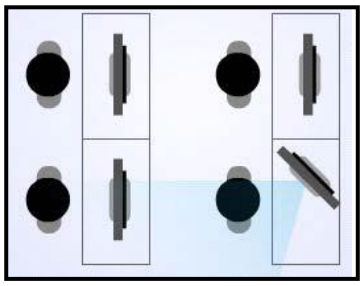
¿Qué medidas se pueden tomar para evitar los virus y otros programas informáticos maliciosos?

- ✓ Ante la sospecha de una infección por virus, debe comunicarse la incidencia de acuerdo con el procedimiento correspondiente. Hay que adoptar todas las precauciones posibles al ejecutar cualquier programa, además de evitar ejecutar archivos adjuntos recibidos por correo electrónico y visitar páginas de Internet con contenidos de legalidad o moralidad dudosas.

MEDIDAS DE SEGURIDAD

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

✓ Las pantallas —especialmente las que estén en zonas con acceso del público— deben orientarse de tal manera que se impida al personal no autorizado el ángulo de visión lo máximo posible.



✓ La información que contenga datos de carácter personal o sea confidencial, independientemente del formato en que esté (dispositivos de almacenamiento, archivadores, pantallas...), debe ser custodiada siempre por el profesional que la tenga a su cargo, para evitar que personas no autorizadas accedan a ella.

× **Nunca debe mantenerse información a la vista** de otras personas sin que la persona que la tiene a su cargo lo controle debidamente. Si va a ausentarse, hay que tomar medidas para evitar que se pueda acceder a la información: por ejemplo, bloquear la sesión del ordenador, guardar las historias clínicas bajo llave, recoger de las impresoras los documentos en el mismo momento en que se imprimen...

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

✓ **Tanto el identificador de usuario o las tarjetas criptográficas como la contraseña correspondiente son confidenciales, personales e intransferibles**. Por tanto, es responsabilidad del titular el uso que haga de ellos.

× En ningún caso deben mantenerse las contraseñas en archivos digitales, escritas en papel o en cualquier otro tipo de soporte legible o accesible.

× **En ninguna circunstancia puede utilizarse una sesión abierta bajo otra identidad.**

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

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

× Cada usuario debe cambiar su contraseña de acceso a los sistemas al menos una vez al año 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 solicitan por teléfono o correo electrónico. Hay que comunicar tal incidencia al Servicio de Atención al Usuario.

✓ Cuando un usuario finalice su relación o vinculación con el Servicio de Salud, la persona directamente responsable de dicho usuario debe comunicar la nueva situación al encargado de la gestión de los usuarios para que dé de baja sus cuentas y autorizaciones.

¿Se pueden usar otros mecanismos de identificación y autentificación?

- ✓ **Sí,** además del sistema basado en el uso de identificadores de usuario y contraseña se pueden usar algoritmos criptográficos y certificados digitales, con los cuales se establecen garantías equivalentes respecto a la autenticación de la identidad de los actores, a la confidencialidad, a la integridad y al no repudio de la información tratada.

- ✓ Se requiere que el usuario use un certificado digital, cuya autenticidad e integridad están garantizadas por un tercero de confianza.

¿Qué es el Servicio de Atención al Usuario?

Es el servicio que presta apoyo informático a los usuarios y gestiona las incidencias que sufran con relación a las aplicaciones y a la infraestructura de las aplicaciones.

EL PUESTO DE TRABAJO

¿Cómo debe estar el puesto de trabajo?

Con carácter general, el puesto de trabajo debe estar despejado, sin más material sobre la mesa que el necesario para 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 en un lugar cerrado (en un cajón o un armario bajo llave) o en una habitación separada y cerrada con llave, al menos fuera del horario de trabajo.

- ✓ 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.

¿Hay que bloquear los terminales, los ordenadores personales y los dispositivos móviles con acceso a la información antes de abandonar el puesto de trabajo?

- ✓ **Sí,** tanto momentáneamente como al final de la jornada laboral. Así mismo, hay que bloquear el puesto de trabajo al cabo de un tiempo de inactividad.

¿Qué es la caracterización del puesto de trabajo?

Es la 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.

USO DE INTERNET Y DEL CORREO ELECTRÓNICO

¿Está permitido conectarse con redes externas al Servicio de Salud?

× **No está permitido** utilizar otros medios de conexión con redes externas sin la autorización correspondiente.

¿Es necesaria la autorización para habilitar conexiones remotas?

✓ Cualquier conexión remota que tenga que habilitarse —a solicitud de un usuario interno o de un proveedor externo— debe tener la autorización previa del responsable correspondiente.

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

× **No,** solo se pueden usar los que están previstos en los estándares. Tampoco se puede modificar la configuración de dichos programas en los aspectos relacionados con la seguridad.

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

× **No.** Como cualquier otro recurso, el navegador o el correo electrónico se pueden usar para uso personal solamente si el usuario está autorizado para ello.

¿Cómo se puede asegurar la confidencialidad de la información que vaya a transmitirse por Internet?

✓ Usando el protocolo HTTPS ("protocolo seguro de transferencia de hipertexto"); debería aparecer en la barra de direcciones del navegador.

✓ También debería aparecer un icono en forma de candado, que informa sobre el certificado digital de identidad de la web visitada.

¿Qué es el correo basura?

Se trata de mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades y que perjudican de alguna manera al receptor.

¿Qué se entiende por *correo electrónico profesional*?

El correo electrónico profesional es un medio de comunicación interpersonal, **no un medio de difusión masiva** e indiscriminada de información.

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

× Todo usuario **debe evitar enviar datos de carácter personal por correo electrónico**. En cualquier caso, solo se pueden transmitir usando mecanismos que garanticen la integridad de los datos y con la autorización correspondiente.

¿Se puede acceder al correo dirigido a otro usuario?

× **Está expresamente prohibido** leer, borrar, copiar o modificar mensajes de correo electrónico o archivos dirigidos a otros usuarios.

¿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 o que contengan virus o códigos malignos.

✓ 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.

¿Qué acciones se consideran como un 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 sonido o vídeo.
- La distribución de virus o troyanos y cualquier actividad encaminada a acceder ilícitamente a otros sistemas de información.
- La piratería de cualquier material multimedia con derecho de la propiedad intelectual.
- El acceso a chats y a juegos en línea.
- La publicación en Internet de información relacionada con el Servicio de Salud, salvo que se tenga la autorización expresa para hacerlo.

¿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?

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

¿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.

INCIDENCIAS EN LA SEGURIDAD

¿Qué es una incidencia?

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

¿En qué circunstancias deben comunicarse las incidencias en la seguridad?

- ✓ A juicio de cada usuario, cualquier incidente que pueda tener impacto en la seguridad y todos los detalles observados que le hayan inducido a sospechar. Por ejemplo, si observa que en el ordenador se producen acciones extrañas: aumento del tamaño de los ficheros, aparición de avisos de Windows no habituales, recepción de correos de personas desconocidas o en idiomas no habituales, pérdidas de datos o de programas…

¿A quién deben notificarse las incidencias en la seguridad?

- ✓ Al servicio de apoyo correspondiente, al cual hay que prestar la colaboración necesaria para resolver la incidencia.

- × La omisión o el retraso en la notificación de un incidente en la seguridad pueden llegar a constituir una falta y, por tanto, dar lugar a la responsabilidad disciplinaria que corresponda.

¿Qué es un activo?

Es un componente o una funcionalidad de un sistema de información susceptible de ser atacados deliberada o accidentalmente 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?

- ✓ Debido a la naturaleza dinámica y cambiante de los requisitos que han de satisfacer, las aplicaciones informáticas deben mantenerse siempre actualizadas. Para ello es imprescindible la colaboración de todos los usuarios y por eso les animamos a comunicar cualquier deficiencia que detecten o las mejoras que consideren adecuadas.

FINALIZACIÓN DE LA VINCULACIÓN O RELACIÓN CON EL SERVICIO DE SALUD

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

- ✓ Devolver cualquier soporte que contenga datos a los que haya tenido acceso en el marco de su vinculación o relación con el Servicio de Salud.
- ✓ Ceder el control sobre cualquier fichero o documento relativo a su prestación profesional.

MONITORIZACIÓN Y APLICACIÓN DEL CÓDIGO

¿Qué acciones llevará a cabo el Servicio de Salud?

Por motivos legales, de seguridad y de calidad del servicio, el Servicio de Salud llevará a cabo las acciones siguientes:

- ✓ Revisará periódicamente el estado de los equipos, de las aplicaciones instaladas, de los dispositivos y de las redes.
- ✓ Monitorizará los accesos a la información contenida en los sistemas.
- ✓ Auditará la seguridad de las credenciales y de las aplicaciones.
- ✓ Monitorizará los servicios de Internet y de correo electrónico y otras herramientas de colaboración.

Esta actividad se llevará a cabo sin usar sistemas o programas que puedan atentar contra los derechos constitucionales de los usuarios.

¿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 desaparezca la causa de la inseguridad o de la degradación.

¿Quién velará para que se cumpla el Código de buenas prácticas?

La Subdirección de la OTIC, con la colaboración del resto de las unidades del Servicio de Salud.