ID	CASTELLANO	CATALÁN
1	Respete el Código de buenas prácticas en el uso de los sistemas de información del Servicio de Salud de las Islas Baleares	Respectau el Codi de bones pràctiques en l'ús dels sistemes d'informació del Servei de Salut de les Illes Balears
2	Atienda siempre las recomendaciones de seguridad	Ateneu sempre les recomanacions de seguretat
3	Infórmese sobre la normativa vigente relativa a la seguridad de la información y cúmplala	Informau-vos sobre la normativa vigent relativa a la seguretat de la informació i compliu-la
4	Guarde el secreto profesional estrictamente y preserve la confidencialidad de la información	Servau el secret professional estrictament i preservau la confidencialitat de la informació
5	Puede proporcionar información con datos de carácter personal solamente a las personas interesadas	Podeu proporcionar dades de caràcter personal només a les persones interessades
6	Si transporta información confidencial o secreta, hágalo con dispositivos cifrados o en sobres cerrados	Si transportau informació confidencial o secreta, feis-ho amb dispositius xifrats o dins sobres tancats
7	Si comparte datos por medio de CD, DVD o USB, asegúrese de que no sean accesibles para personas no autorizadas y de que son borrados o destruidos después de usarlos	Si compartiu dades per mitjà de CD, DVD o USB, assegurau-vos que no siguin accessibles per a persones no autoritzades i que són esborrats o destruïts després d'emprarlos
8	No use sistemas de información distintos a los que proporciona el Servicio de Salud de las Islas Baleares	No empreu sistemes d'informació diferents als que proporciona el Servei de Salut de les Illes Balears
9	Evite generar archivos temporales. Si lo hace, elimínelos al terminar de usarlos	Evitau generar fitxers temporals. Si ho feis, eliminau-los quan acabeu d'emprar-los
10	No proporcione información personal por teléfono o correo electrónico a personas no autorizadas	No proporcioneu informació personal per telèfon o correu electrònic a persones no autoritzades
11	Conserve la documentación confidencial en cajones o armarios bajo llave	Conservau la documentació confidencial dins calaixos o armaris tancats amb clau
12	Proteja las zonas de acceso restringido	Protegiu les zones d'accés restringit
13	Destruya de forma segura la documentación que contenga información confidencial	Destruïu de manera segura la documentació que contengui informació confidencial
14	No modifique la configuración de seguridad establecida en los sistemas	No modifiqueu la configuració de seguretat establerta en els sistemes
15	No saque ningún equipo de las instalaciones del Servicio de Salud, excepto si tiene autorización para hacerlo	No tragueu cap equip de les instal·lacions del Servei de Salut, llevat que tingueu autorització per fer-ho
16	No se conecte a redes ni a sistemas externos por otros medios que no sean los definidos y administrados por el personal informático competente	No us connecteu a xarxes ni a sistemes externs per altres mitjans que no siguin els definits i administrats pel personal informàtic competent
17	No extraiga ni use información confidencial o datos de carácter personal en entornos que no estén protegidos o configurados adecuadamente	No extraieu ni empreu informació confidencial o dades de caràcter personal en entorns que no estiguin protegits o configurats adequadament

18	No traslade fuera de las instalaciones habituales de trabajo datos o información sin la autorización correspondiente	No traslladeu fora de les instal·lacions habituals de feina dades o informació sense l'autorització corresponent
19	Solamente puede acceder a los sistemas requeridos para desempeñar las funciones que tenga asignadas	Només podeu accedir als sistemes requerits per acomplir les funcions que tingueu assignades
20	No utilice los recursos informáticos para fines privados, ya que son una herramienta de trabajo y tienen una capacidad limitada	No utilitzeu els recursos informàtics per a finalitats privades, ja que són una eina de treball i tenen una capacitat limitada
21	Si sospecha de un incidente de seguridad, notifíquelo inmediatamente al Centro de Atención de Usuarios (CAU)	Si sospitau d'un incident de seguretat, notificau-ho immediatament al Centre d'Atenció d'Usuaris (CAU)
22	No abra archivos adjuntos que haya recibido de correos sospechosos o de los que desconozca su procedencia	No obriu fitxers adjunts que hàgiu rebut d'adreces sospitoses o si en desconeixeu la procedència
23	No visite páginas web de contenidos de moralidad o legalidad dudosa	No visiteu pàgines web de continguts de moralitat o legalitat dubtosa
24	Oriente su monitor de manera que evite al máximo que lo vean personas no autorizadas, especialmente si trabaja en una zona con acceso de público	Orientau el monitor de manera que eviteu al màxim que el vegin persones no autoritzades, especialment si feis feina en una zona amb accés de públic
25	Custodie en todo momento la información que contenga datos de carácter personal o sea confidencial, independientemente del formato en que esté (dispositivos de almacenamiento, archivadores, pantallas…), a fin de evitar que personas no autorizadas accedan a ella	Custodiau sempre la informació que contengui dades de caràcter personal o sigui confidencial, independentment del format en què estigui (dispositius d'emmagatzematge, arxivadors, pantalles…), a fi d'evitar que persones no autoritzades hi accedeixin
26	Bloquee el ordenador siempre que vaya a abandonar su puesto de trabajo	Blocau l'ordinador sempre que hàgiu d'abandonar el lloc de feina
27	Recuerde que sus credenciales de acceso son confidenciales, personales e intransferibles. El uso que se haga de ellas será responsabilidad suya	Recordau que les vostres credencials d'accés són confidencials, personals i intransferibles. L'ús que se'n faci serà responsabilitat vostra
28	No debe utilizar una sesión abierta con otra identidad	No heu d'utilitzar una sessió oberta amb una altra identitat
29	Si sospecha que hay personas no autorizadas que saben su contraseña de manera fortuita o fraudulenta, modifíquela y comuníquelo al CAU inmediatamente	Si sospitau que hi ha persones no autoritzades que saben la vostra contrasenya de manera fortuïta o fraudulenta, modificau-la i comunicau-ho al CAU immediatament
30	Al crear una contraseña, procure que otras personas no puedan adivinarla fácilmente	En crear una contrasenya, procurau que altres persones no puguin endevinar-la fàcilment
31	La omisión o el retraso en la notificación de un incidente de seguridad puede llegar a constituir una falta y, por tanto, derivar en la responsabilidad disciplinaria que corresponda	L'omissió o el retard a l'hora de notificar un incident de seguretat pot arribar a constituir una falta i, per tant, derivar en la responsabilitat disciplinària que hi escaigui

32	Comunique cualquier deficiencia que detecte o cualquier mejora que considere adecuada sobre los cambios en las aplicaciones informáticas	Comunicau qualsevol deficiència que detecteu o qualsevol millora que considereu adequada sobre els canvis en les aplicacions informàtiques
33	Cualquier conexión remota que tenga que habilitarse debe estar autorizada previamente por el responsable correspondiente. Además, la autorización debe tener la validación del servicio de informática a fin de garantizar los niveles de seguridad requeridos	Qualsevol connexió remota que s'hagi d'habilitar ha d'estar autoritzada prèviament pel responsable corresponent. A més, l'autorització ha de tenir la validació del servei d'informàtica a fi de garantir els nivells de seguretat requerits
34	No puede publicar en Internet información relacionada con el Servicio de Salud de las Islas Baleares, salvo en los casos en que tenga autorización expresa para hacerlo	No podeu publicar a Internet informació relacionada amb el Servei de Salut de les Illes Balears, excepte en els casos en què tingueu autorització expressa per fer-ho
35	El correo electrónico es un medio de comunicación interpersonal, no un medio de difusión masiva e indiscriminada de información	El correu electrònic és un mitjà de comunicació interpersonal, no un mitjà de difusió massiva i indiscriminada d'informació
36	Está totalmente prohibido leer, borrar, copiar o modificar mensajes de correo electrónico o archivos dirigidos a otras personas	Està totalment prohibit llegir, esborrar, copiar o modificar missatges de correu electrònic o fitxers adreçats a altres persones
37	El Código de buenas prácticas está a disposición de todo el personal del Servicio de Salud en su sede electrónica y en la intranet corporativa	El Codi de bones pràctiques és a la disposició de tot el personal del Servei de Salut a la seva seu electrònica i a la intranet corporativa
38	Colabore para permitir el ejercicio de los derechos de acceso, rectificación, cancelación y oposición atendiendo de forma correcta y adecuada a las personas interesadas e informándolas sobre el procedimiento que tienen que seguir	Col·laborau per permetre l'exercici dels drets d'accés, rectificació, cancel·lació i oposició atenent de manera correcta i adequada les persones interessades i informant-les sobre el procediment que han de seguir
39	La información almacenada localmente en el ordenador personal de cada usuario no se guarda por medio de ningún procedimiento corporativo de copia de seguridad	La informació emmagatzemada localment a l'ordinador personal de cada usuari no es desa per mitjà de cap procediment corporatiu de còpia de seguretat
40	No está permitido hacer copias de los programas instalados en los ordenadores	No és permès fer còpies dels programes instal·lats en els ordinadors
41	Tiene que facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento	Heu de facilitar al personal de suport tècnic l'accés als vostres equips per a tasques de reparació, instal·lació o manteniment
42	Los ordenadores personales de la organización deben mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Por ello tiene que prestar especial atención a la actualización, la configuración y el funcionamiento correctos de los programas antivirus y cortafuegos	Els ordinadors personals de l'organització han de mantenir actualitzats els pegats de seguretat de tots els programes que tenguin instal·lats. Per això heu de prestar especial atenció a l'actualització, la configuració i el funcionament correctes dels programes antivirus i tallafocs

43	No puede conectar a la red informática de comunicaciones corporativa ningún dispositivo distinto a los configurados, habilitados y admitidos por el Servicio de Salud	No podeu connectar a la xarxa informàtica de comunicacions corporativa cap dispositiu diferent dels configurats, habilitats i admesos pel Servei de Salut
44	Los dispositivos personales usados en el ámbito del Servicio de Salud que accedan a sus redes y aplicaciones pueden ser sometidos a actividades de prevención y control	Els dispositius personals emprats en l'àmbit del Servei de Salut que accedeixin a les seves xarxes i aplicacions poden ser sotmesos a activitats de prevenció i control
45	No está permitido transmitir o alojar información sensible o confidencial ni datos de carácter personal o información protegida propia del Servicio de Salud en servidores externos o soluciones de almacenamiento en la nube, salvo que esté autorizado expresamente	No és permès transmetre o allotjar informació sensible o confidencial ni dades de caràcter personal o informació protegida pròpia del Servei de Salut en servidors externs o solucions d'emmagatzematge en el núvol, llevat que estigui autoritzat expressament
46	Si recibe una llamada telefónica o un mensaje electrónico en que se le pida su identificador de usuario y/o su contraseña, no los facilite bajo ningún concepto y notifíquelo inmediatamente al Centro de Atención al Usuario (CAU)	Si rebeu una telefonada o un missatge electrònic en què us demanin el vostre identificador d'usuari i/o la contrasenya, no els faciliteu de cap manera i notificau-ho immediatament al Centre d'Atenció a l'Usuari (CAU)
47	Cuando termine su relación o vinculación con un puesto o una función determinados que tenga asociados medios informáticos o de comunicaciones proporcionados por el Servicio de Salud, debe devolverlos inmediatamente a la unidad responsable	Quan acabeu la relació o vinculació amb un lloc o una funció determinats que tengui associats mitjans informàtics o de comunicacions proporcionats pel Servei de Salut, heu de tornar-los immediatament a la unitat responsable
48	El sistema puede registrar y dejar traza de las páginas a las que haya accedido y del tiempo de acceso y del volumen de los archivos descargados	El sistema pot registrar i deixar traça de les pàgines a les quals hàgiu accedit i del temps d'accés i del volum dels fitxers descarregats
49	El Servicio de Salud revisa periódicamente el estado de los equipos, de los programas instalados, de los dispositivos y de las redes de comunicaciones de su responsabilidad	El Servei de Salut revisa periòdicament l'estat dels equips, dels programes instal·lats, dels dispositius i de les xarxes de comunicacions que són responsabilitat seva
50	Los sistemas en los que se detecte un uso inadecuado o no se cumplan los requisitos mínimos de seguridad pueden ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando se haya eliminado la causa de la inseguridad o degradación	Els sistemes en els quals es detecti un ús inadequat o no es compleixin els requisits mínims de seguretat poden ser blocats o suspesos temporalment. El servei es restablirà quan s'hagi eliminat la causa de la inseguretat o degradació

51	El Servicio de Salud no emprenderá nunca ninguna actividad de monitorización utilizando sistemas o programas que puedan atentar contra los derechos constitucionales de los usuarios —como el derecho a la intimidad personal y al secreto de las comunicaciones—, de forma que se mantendrá en todo momento la privacidad de la información manejada	El Servei de Salut no emprendrà mai cap activitat de monitoratge utilitzant sistemes o programes que puguin atemptar contra els drets constitucionals dels usuaris —com ara el dret a la intimitat personal i al secret de les comunicacions—, de manera que es mantindrà sempre la privadesa de la informació manejada
52	El Servicio de Salud de las Islas Baleares tiene una política de seguridad en la que se establecen los objetivos y las funciones en esta materia	El Servei de Salut de les Illes Balears té una política de seguretat en la qual s'estableixen els objectius i les funcions en aquesta matèria
53	El documento sobre la política de seguridad está a disposición de todo el personal del Servicio de Salud en su sede electrónica y en la intranet corporativa	El document sobre la política de seguretat és a disposició de tot el personal del Servei de Salut a la seva seu electrònica i a la intranet corporativa