




ESQUEMA NACIONAL DE SEGURIDADE


**FUNCIÓNS E RESPONSABILIDADES DO
PERSOAL EN RELACIÓN AO TRATAMENTO
DE DATOS PERSOAIS**

ENS.DOC.SEG.07-02

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 2


CONTROL DO DOCUMENTO

Referencia		Nome do Documento	Clasificación
ENS.DOC.SEG.07-02		Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	Oficial - Interno
Versión	Data	Propósito/descrición do cambio	Data revisión
1.0	05/12/2024		
Autor			
Oficina de Seguridade da Información			
Aprobado por			Data aprobación
Comité de Seguridade da Información			18/12/2024
Control de versións			
O Responsable de Seguridade da Información é o responsable do control de versións deste documento.			
Control de Calidade			
O Comité de Seguridade da Información é responsable da revisión do Documento, no marco do seguimento periódico da Política de Seguridade da Información, ou como consecuencia de cambios significativos propostos no marco das auditorías de seguridade.			

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 3

INDICE

1. OBXECTO:.....	4
2. ALCANCE	4
3. ORGANIZACIÓN DA PROTECCIÓN DE DATOS PERSOAIS NA USC.....	4
4. ROLES DO PERSOAL.....	5
4. 1. Roles implicados na organización da seguridade da información na USC.....	5
4. 2. Roles complementarios.....	5
5. NORMATIVA APLICABLE.....	6
6. FUNCIÓNS E RESPONSABILIDADES EN RELACIÓN AOS TRATAMENTOS DE DATOS PERSOAIS.....	6
6.1. Obrigas xerais.....	6
6.2. Uso persoal e intransferible das credenciais de acceso	7
6.3. Protección do posto físico de traballo	7
6.4. Uso de ficheiros de traballo con datos persoais	8
6.5. Utilización de soportes.....	8
6.6. Traballo fóra dos locais universitarios	9
6.7. Comunicación de incidencias.....	9
6.8. Envío de datos por medio de redes de comunicacións	9
7. FUNCIÓNS E RESPONSABILIDADES DAS ENTIDADES OU PERSOAS ENCARGADAS DO TRATAMENTO	10
8. DOCUMENTOS RELACIONADOS.....	10

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 4

1. OBXECTO:

Este documento define as funcións e responsabilidades do persoal ao servizo da USC así como o de empresas ou organismos colaboradores, no relativo ao tratamento de datos persoais.

2. ALCANCE

As instrucións contidas neste documento afectan a todo o persoal da USC que realice tratamentos de datos persoais, automatizados ou non automatizados.

Tamén afecta ás persoas traballadora de empresas ou organismos que traten datos persoais contidos en tratamentos cuxo responsable sexa a USC como consecuencia dun contrato de encargado de tratamento.

3. ORGANIZACIÓN DA PROTECCIÓN DE DATOS PERSOAIS NA USC

Para a prestación do servizo público de ensinanza superior propio da USC deben ser tratados datos persoais.


Nesta materia xorden varias responsabilidades a nivel legal ou organizativo:

a) **Responsable do tratamento.** É a persoa física ou xurídica, autoridade pública, servizo ou organismo que, só ou xunto con outros, determine os fins e medios do tratamento, neste caso, a Universidade de Santiago de Compostela.

b) **Encargado do tratamento.** É a persoa física ou xurídica, autoridade pública, servizo ou organismo que trate datos por conta do responsable do tratamento. A relación entre responsable e encargado deberá estar regulada nun contrato, convenio ou outro instrumento xurídico.

c) **Delegada ou Delegado de protección de datos.** De conformidade co Regulamento Xeral de Protección de Datos, nos artigos 37 ao 39, debe cumprir cos seguintes requisitos, características e funcións:

- Ser un ou unha profesional que poida acreditar formación e coñecementos especializados en materia de protección de datos. Poderá establecerse a través de contratación externa ou mediante designación dentro do cadro de persoal da organización.
- Asegurar o cumprimento normativo da protección de datos, facendo compatible o funcionamento da organización, a consecución dos obxectivos lícitos e lexítimos da súa actividade e a garantía do dereito á protección de datos e coa seguridade da información.
- Ser interlocutor necesario coa Autoridade de Control da Protección de Datos.
- Informar e asesorar á persoa responsable e/ou encargada do tratamento e ás persoas empregadas da USC que se ocupen do tratamento dos datos persoais, das obrigas que lles incumben en virtude do Regulamento e outras disposicións de protección de datos da Unión ou do Estado Español.
- Supervisar o cumprimento do disposto no Regulamento e noutras disposicións de protección de datos da Unión e das políticas da persoa responsable ou encargada do tratamento en materia de

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 5

protección de datos persoais, incluída a asignación de responsabilidades, a concienciación e a formación do persoal que participa nas operacións de tratamento.

- Supervisar a realización das auditorías correspondentes.
- Ofrecer o asesoramento que se lle pida acerca da avaliación de impacto relativa á protección de datos e supervisar a súa realización.
- Cooperar e actuar en contacto coa autoridade de control, neste caso a Axencia Española de Protección de Datos, para as cuestións relacionadas co tratamento de datos persoais, incluída a consulta previa e calquera outro tipo de consulta.

Dentro da Política de Seguridade da Información, terá as seguintes funcións e prerrogativas:

- Ser oída ou oído en todos os aspectos relacionados coa seguridade dos datos persoais e violacións de seguridade, desde a perspectiva da confidencialidade, integridade e dispoñibilidade.
- Participar, como invitado permanente, nas reunións do Comité de Seguridade da información.
- Emitir o seu parecer nos aspectos relacionados coa seguridade dos datos persoais, promover, no seu caso, revisións de análise de riscos e de avaliacións de impacto en protección de datos; elaboración ou modificación, entre outros, de procedementos ou políticas de seguridade de datos persoais.
- Promover accións de formación e concienciación en privacidade.
- En xeral, todas as funcións que teñan que ver coa protección de datos na entidade.

d) **Secretaría Xeral.** Corresponde a este órgano a posta en marcha da política de protección de datos e a xestión dos seus procedementos.

4. ROLES DO PERSOAL


4. 1. Roles implicados na organización da seguridade da información na USC

- a) Responsable da información ou Responsable do tratamento
- b) Responsable dos servizos
- c) Responsable da seguridade da información
- d) Responsable dos sistemas

As persoas que exerzan estes roles terán as funcións e responsabilidades que se determinan na Política de Seguridade da Información da USC.

4. 2. Roles complementarios

- Consideraranse **persoas usuarias** todas as persoas que teñen acceso aos datos persoais a través de documentos, ficheiros ou aplicacións informáticas como consecuencia das tarefas que en función do seu posto de traballo, teñen encomendadas.
- A **encargada do tratamento** será a Universidade de Santiago de Compostela. O órgano encargado da Protección de Datos será a Secretaría Xeral, que poderá designar subencargados/as de tratamento.
- **Outros colectivos:** Son as persoas do cadro do persoal da USC ou de empresas alleas que con motivo do seu desempeño profesional poidan potencialmente ter acceso a información de carácter persoal.

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 6

5. NORMATIVA APLICABLE

Ademais das funcións relativas ao desempeño profesional asociado ao seu posto de traballo, todo o persoal debe cumprir a seguinte normativa:

- Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, (Regulamento xeral de protección de datos, RGPD).
- Lei orgánica 3/2018, do 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais (LOPDGDD).
- Regulamento sobre o uso das TIC na USC
- Política de privacidade e protección de datos persoais na USC
- Rexistro de tratamentos da USC
- Protocolo sobre o uso de instalacións de videovixilancia da USC
- Política de Seguridade da Información da USC
- Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade, así como a normativa e procedementos desenvolvidos pola USC para este fin.


Todos os usuarios colaborarán co responsable do tratamento e co responsable de seguridade a prol de velar polo cumprimento da lexislación e da regulamentación vixente que afecte á materia de protección de datos.

6. FUNCIÓNS E RESPONSABILIDADES EN RELACIÓN AOS TRATAMENTOS DE DATOS PERSOAIS

Todas as persoas usuarias teñen as seguintes obrigas en relación co tratamento de datos persoais:

6.1. Obrigas xerais

- Gardar segredo profesional e confidencialidade da información tratada. Quen interveña en calquera fase dun expediente en que se realice tratamento dos datos persoais está obrigado ao segredo profesional respecto deles, obriga que subsistirá aínda despois de finalizar a súa relación coa USC. A vulneración do deber de gardar segredo sobre os datos persoais será considerada como unha falta leve, grave ou moi grave de conformidade co previsto na normativa vixente, o que poderá dar lugar á iniciación de actuacións disciplinarias.
- Utilizar os sistemas de información, recursos técnicos e a información persoal á que accede unicamente para o desempeño da súa actividade profesional.
- Acceder exclusivamente a aqueles datos ou recursos que se precisen para o desenvolvemento das súas funcións. O acceso a outros datos deberá ser autorizado expresamente.
- Acceder aos sistemas da USC dende o exterior cumprindo coas especificacións técnicas que se determinen en cada momento para manter unha conexión segura (VPN e/ou calquera outro programa ou protocolo que a universidade estime que debe utilizarse para conexións externas).
- Facilitar os dereitos en materia de protección de datos ás persoas titulares deles. As persoas titulares dos datos poderán exercer os seus dereitos en materia de protección de datos

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 7

empregando os formularios habilitados para os efectos, que estarán a súa disposición na Sede Electrónica da USC.

- Comunicar á Secretaría Xeral calquera petición de datos realizada por terceiras persoas, polas forzas ou corpos de seguridade do Estado, pola Fiscalía e por calquera xulgado.

6.2. Uso persoal e intransferible das credenciais de acceso

Cada persoa usuaria será responsable da confidencialidade do seu contrasinal e, no caso de que este sexa coñecida fortuíta ou fraudulentamente por persoas non autorizadas, deberá notificalo ao Centro de Atención a Usuarios, procedendo inmediatamente ao seu cambio.


Observaranse as disposicións vixentes na USC ao respecto (NOSI-002-Xestión e utilización de credenciais) e, concretamente, as seguinte obrigas:

- Cada persoa usuaria deberá cambiar a chave de paso inicial que se lle asigne no primeiro acceso que realice, naqueles casos en que fose necesaria a intervención doutras persoas no proceso de xeración e distribución da mesma.
- Os contrasinais de acceso deberán ser suficientemente complexos para que sexan dificilmente deducibles por terceiras persoas, evitando o uso do propio identificador, palabras sinxelas ou que poidan relacionarse coa persoa usuaria.
- Os requisitos que deben cumprir os contrasinais recóllense pola Área TIC na páxina: <https://www.usc.gal/gl/servizos/area/tecnoloxias-informacion-comunicacions/servizos/identidade/recomendacions-seguridade>

A USC poderá establecer de xeito obrigatorio o uso do dobre factor de autenticación para acceder aos sistemas que conteñan datos persoais.

6.3. Protección do posto físico de traballo

- Cada posto físico de traballo estará baixo a responsabilidade da persoa usuaria autorizada. Esta deberá custodiar a documentación e garantir que a información que amosa non sexa visible a persoas non autorizadas.
- As pantallas, impresoras e outro tipo de dispositivos conectados ao posto de traballo deberán estar fisicamente situados en lugares que garantan esa confidencialidade.
- Cando a persoa responsable dun posto de traballo o abandone, ben temporalmente ou ben ao finalizar a súa quenda de traballo, deberá deixalo nun estado que impida a visualización dos datos protexidos como por exemplo un protector de pantalla con contrasinal. A continuación do traballo implicará a desactivación da pantalla protectora coa introdución do contrasinal correspondente. Do mesmo xeito, asegurarse de que non quedan no seu posto documentos físicos ou outros soportes que conteñan datos persoais aos que poidan acceder persoas non autorizadas.
- No caso das impresoras, deberá asegurarse de que non quedan documentos que conteñan datos protexidos na bandexa de saída. Se son compartidas con outras persoas usuarias non autorizadas para acceder aos datos persoais, as persoas responsables de cada posto deberán retirar os documentos conforme saian da impresora.

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 8

- Os borradores ou copias mal impresas deberán ser destruídas de tal xeito que non quede rastro dos datos persoais, conforme á disposición “ENS.PO.SEG.05 – Procedemento de xestión de soportes”.
- Queda expresamente prohibido calquera cambio da configuración da conexión dos postos de traballo a redes ou sistemas exteriores que non estean autorizados expresamente pola persoa responsable do tratamento ou polas persoas administradoras do sistema. A revogación desta prohibición deberá ser autorizada expresamente.
- Os postos de traballo dende os que se ten acceso aos datos persoais terán unha configuración fixa nas súas aplicacións e sistemas operativos que só poderá ser cambiada por autorización da persoa responsable do tratamento ou das persoas administradoras do sistema.
- No caso de categorías especiais de datos [*datos que revelen a orixe étnica ou racial, opinión políticas, conviccións relixiosas ou filosóficas, afiliación sindical, datos xenéticos, datos biométricos dirixidos a identificar de maneira unívoca a unha persoa física, datos relativos á saúde ou á vida sexual ou ás orientación sexuais*], os datos deberán estar baixo o control do responsable do tratamento. No caso de ser estritamente necesario copiar ou utilizar estes datos en dispositivos móbiles ou extraíbles fóra das instalacións da USC deberanse cifrar sempre. Se isto non fose posible, comunicarse ao responsable de seguridade da información para que tome as medidas alternativas que procedan.

6.4. Uso de ficheiros de traballo con datos persoais


No caso de ter que utilizar arquivos de traballo que conteñan datos persoais fóra do ámbito das bases de datos centralizadas, deberanse adoptar as seguintes precaucións:

- Utilizar exclusivamente as ferramentas ofimáticas postas a disposición pola USC.
- Xerar os ficheiros na nube da USC.
- No caso de ter que utilizar unha copia nun ordenador local, deberán realizarse as copias sempre nun mesmo cartafol de xeito que non queden dispersas por todo o disco do ordenador.
- Tras realizar o tratamento para o que foran necesarios eses datos temporais, proceder ao seu borrado total.
- Os tratamentos creados exclusivamente para a realización de traballos temporais ou auxiliares deberán cumprir coas mesmas medidas de seguridade que o tratamento orixinal.

6.5. Utilización de soportes

As persoas ao servizo da USC non utilizarán sistemas extraíbles que conteñan datos persoais, debendo utilizar as aplicacións corporativas ou a nube da USC para o acceso aos datos necesarios para o seu traballo ordinario. Non obstante o anterior, no caso de ser imprescindible o seu uso deberá comunicarse á persoa responsable do tratamento a existencia de soportes, para que proceda ao seu inventariado e etiquetaxe, segundo o procedemento vixente.

Cando unha persoa usuaria xestione ou produza soportes que conteñan datos persoais, ben como consecuencia de operacións intermedias propias da aplicación que os trata, ou ben como consecuencia de procesos periódicos de copiado de seguridade ou calquera outra operación esporádica, estes deberán estar claramente identificados cunha etiqueta externa.

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 9

Os soportes que conteñan datos persoais deberán ser almacenados en lugares aos que non teñan acceso persoas non autorizadas.

A saída de soportes fóra dos locais previstos para o traballo habitual deberá ser expresamente autorizada polo responsable do tratamento.

Os documentos de traballo e soportes informáticos que se xeren por mor dun tratamento e teñan que desbotarse deberán ser destruídos tras o seu uso seguindo a disposición “ENS.PO.SEG.05 – Procedemento de xestión de soportes”.

Cando se reciclen medios que sexan reutilizables e que contivesen copias de datos persoais, deberán ser borrados fisicamente antes da súa reutilización de xeito que os datos que contiñan non sexan recuperables.

6.6. Traballo fóra dos locais universitarios

Os traballos que impliquen tratamento de datos persoais fóra dos locais da USC deberán de ser expresamente autorizados.

Non se deberá copiar nin transportar información dos sistemas centrais en dispositivos móbiles (memorias USB, discos duros externos, teléfonos móbiles, táboas dixitais, CD, DVD ou similares) sen a correspondente autorización.

O acceso remoto ao ficheiro e a datos persoais deberá estar expresamente autorizado e deberá realizarse a través de canles seguras postas a disposición pola USC.

6.7. Comunicación de incidencias

Calquera persoa usuaria que teña coñecemento dunha incidencia deberá comunicala á persoa responsable do tratamento, á persoa responsable de seguridade ou á persoa inmediatamente superior na liña xerárquica, segundo o procedemento “ENS.PO.SEG.04 – Procedemento de xestión de incidencias e fendas de seguridade”.


O coñecemento e non notificación de incidencias por parte da persoa usuaria será considerada como unha falta contra a seguridade do tratamento pola súa parte.

6.8. Envío de datos por medio de redes de comunicacións

Non se deberán realizar envíos que conteñan listaxes de datos persoais a correos alleos á USC, agás autorización da persoa responsable do tratamento. Do mesmo xeito, só quen teña autorización poderá facer transferencias electrónicas de datos persoais, utilizando as ferramentas máis seguras dispoñibles en cada momento.

No caso de categorías especiais de datos toda a información que se transmita deberá ser autorizada e deberase cifrar a información do seguintes elementos:

- Os soportes físicos que deban ser enviados fóra das instalacións que estean baixo o control da persoa responsable do tratamento.

	DOCUMENTOS: Funcións e responsabilidades do persoal en relación ao tratamento de datos persoais	CÓDIGO ENS.DOC.SEG.07-02	VERSIÓN 1
		DATA 18/12/2024	PÁXINA 10

- As unidades daqueles ordenadores portátiles que vaian ser utilizados fóra das instalacións que estean baixo o control da persoa responsable do tratamento. Se isto non fose posible, informárase puntualmente á persoa responsable do tratamento.
- As transmisións de datos que circulen a través de redes públicas de telecomunicacións ou sen fíos, como sucede en envíos por correo electrónico fóra dos dominios da USC.
- En todas as transferencias electrónicas de datos persoais incluírase un aviso para quen os vaia recibir no que se sinala a confidencialidade da información e os deberes e usos da información facilitada.

7. FUNCIÓNS E RESPONSABILIDADES DAS ENTIDADES OU PERSOAS ENCARGADAS DO TRATAMENTO

Cando se realice un tratamento de datos por conta da USC deberase asinar o correspondente acordo xurídico no que se plasme o encargo e as condicións de realización, de conformidade cos modelos que establece a USC.

As entidades ou persoas encargados do tratamento ou nas que delegue (subencargado do tratamento) establecidas no acordo, terán as seguintes funcións e obrigas:

- Cando preste servizos nos seus propios locais, corresponderalle á persoa encargada do tratamento elaborar o documento de seguridade do tratamento afectado.
- No caso de servizos prestados nos locais da USC, a persoa encargada do tratamento e todo o persoal ao seu cargo deberá cumprir as normas deste documento de seguridade.
- Cando os tratamentos se procesen en locais de ambas partes, a persoa encargada facilitará á persoa responsable do tratamento a documentación necesaria para concretar, coordinar ou completar o documento de seguridade da USC.
- Cando a persoa encargada do tratamento utilice accesos remotos a sistemas propiedade da USC, deberá obter o consentimento explícito para incorporar datos a sistemas ou soportes propios.
- A persoa encargada de tratamento deberá asumir todas as obrigas propias dos responsables do tratamento, agás as autorizacións de acceso de persoas usuarias ou nomeamentos de persoas responsables delegadas.
- En particular deberá cumprir todas as normas relacionadas coa contorna física, sistema operativo e comunicacións, sistemas informáticos ou aplicacións de acceso ao tratamento, traballo fóra dos locais, xestión de soportes, entrada e saída de datos por rede, procedementos de copia de seguridade e recuperación e, en xeral, todas as incluídas neste documento que afecten á contorna da súa responsabilidade.

8. DOCUMENTOS RELACIONADOS

- POSI-OO1: Política de Seguridade da Información
- NOSI-002: Xestión e utilización de credenciais
- ENS.PO.SEG.04: Procedemento de xestión de incidencias e brechas de seguridade
- ENS.PO.SEG.05: Procedemento de xestión de soportes