

ANEXO III

POLÍTICA XERAL DE PROTECCIÓN DE DATOS

1. Política xeral de protección de datos

1. A Universidade de Santiago de Compostela (USC) é consciente da importancia e necesidade de garantir a privacidade dos datos de carácter persoal dos membros de súa comunidade e, en xeral, de todos os usuarios dos sistemas de información da institución, e con esa finalidade adoptará as medidas técnicas e organizativas necesarias para protexelos, en aplicación da Lei orgánica 15/1999, de 13 de decembro, de protección de datos de carácter persoal, o Real Decreto 1332/1994, de 20 de xuño, o Real Decreto 994/1999, de 11 de xuño, e o resto do ordenamento xurídico.

2. O datos persoais utilizaranse unicamente para as finalidades para as que foron recollidos, en relación coas actividades da Universidade. A cesión de datos de carácter persoal farase na forma e coas limitacións e dereitos establecidos na Lei orgánica 15/1999, de 13 de decembro, de protección de datos de carácter persoal (LOPD). Sen prexuízo do previsto nas disposicións legais e do cumprimento dos fins da Universidade, a USC comprométese a non ceder datos a ningunha entidade ou organismo non previstos no ficheiro de creación sen o consentimento da persoa interesada.

2. Uso e finalidades dos datos de carácter persoal

1. Os datos persoais recollidos pola USC poderán ser incorporados a unha base de datos automatizada e sometidos a tratamento con finalidades académicas e de xestión da USC, e para a difusión de información institucional e de información destinada á formación e á inserción laboral e profesional dos membros da comunidade universitaria.

2. A Universidade poderá facer uso dos datos contidos nos seus ficheiros con finalidades históricas, estatísticas ou científicas.

3. Cesión de datos

Non se fará ningunha cesión de datos de carácter persoal sen consentimento do titular dos datos, agás segundo o previsto pola lei e o declarado pola USC.

4. Ficheiros da Universidade de Santiago de Compostela

Son ficheiros da USC os declarados polas Resolucións reitorais do 24 de xuño de 2002 (DOG do 9 de agosto de 2002) e do 1 de xuño de 2004 (DOG do 28 de xuño de 2004) polas que se crean ficheiros de datos de carácter persoal da Universidade de Santiago de Compostela, así como os que poidan establecerse en aplicación da normativa de protección de datos de carácter persoal.

5. Responsables dos ficheiros

1. Os responsables dos ficheiros son os que figuran sinalados en cada ficheiro e ante eles poderanse exercer os dereitos que establece a LOPD.

2. Os xefes de cada servizo ou unidade que, para cumprimento das súas tarefas administrativas, necesiten tratar datos de carácter persoal serán responsables internos dos arquivos no ámbito da súa función e deberán velar para que o tratamento se axuste en todo momento ao previsto na lei así como asegurarse do establecemento e cumprimento das disposicións de seguridade adecuadas.

6. *Exercicio dos dereitos*

1. As persoas das que a USC teñan datos de carácter persoal poderán exercer os dereitos de acceso, rectificación, cancelación e, no seu caso, oposición, de acordo coa LOPD. Estes dereitos só pode exercelos a persoa afectada ou o seu representante legal cando o afectado fose menor de idade ou declarado incapaz para o exercicio dos seus dereitos.

2. Os dereitos de acceso, rectificación, cancelación e oposición de ficheiros poderán exercerse por medio dun escrito dirixido ao responsable do ficheiro onde se identifique o solicitante, axuntando unha fotocopia do DNI, a petición concreta, o domicilio, e a documentación acreditativa correspondente. A Secretaría Xeral aprobará os modelos de solicitudes para exercer os devanditos dereitos.

3. Posteriormente á recepción no rexistro de entrada do escrito do interesado e á posterior remisión ao órgano a quen vaia dirixido, os responsables internos dos arquivos afectados, unha vez comprobada a pertinencia da solicitude, deberán adoptar as medidas oportunas para satisfacer a petición, cando proceda, e notificar os resultados á persoa interesada.

4. A coordinación e garantía do exercicio destes dereitos correspóndelle á Secretaría Xeral da USC.

7. *Dereito de acceso*

1. O dereito de acceso permite obter información dos datos de carácter persoal sometidos a tratamento, a orixe destes datos e as comunicacións realizadas ou que se prevé facer. Este dereito soamente poderá ser exercido en intervalos non inferiores a doce meses, a non ser que a persoa interesada acredite un cambio de circunstancias ou interese lexítimo.

2. O dereito de acceso poderá denegarse motivadamente por razóns de interese público para salvaguardar dereitos ou intereses de terceiros máis dignos de protección. O afectado a quen se lle denegan estes dereitos poderá poñelo en coñecemento do director da Axencia Española de Protección de Datos, que decidirá sobre a procedencia ou improcedencia da denegación.

3. O responsable do ficheiro resolverá a petición de acceso no prazo máximo dun mes a contar desde a recepción da solicitude.

8. *Dereitos de rectificación e cancelación*

1. Os dereitos de rectificación e cancelación permiten instar ao responsable do ficheiro a cumprir a obriga de manter a exactitude dos datos, rectificando ou cancelando os datos de carácter persoal cando resulten incompletos, inexactos, inadecuados, excesivos ou non axustados ao tratamento disposto pola lei.

2. Cando os datos rectificados ou cancelados foran cedidos previamente, o responsable do ficheiro deberá notificar a rectificación e cancelación efectuada ao cesionario.

3. A cancelación supón o bloqueo dos datos ou, se fose posible, o seu borrado físico. Non obstante, os datos de carácter persoal deberán ser conservados durante os prazos previstos nas disposicións aplicables ou, no seu caso, nas relacións contractuais entre a persoa ou entidade responsable do tratamento e a persoa interesada.
4. A solicitude de rectificación debe indicar o dato que é erróneo e a corrección que debe realizarse e debe estar acompañada da documentación xustificativa da rectificación solicitada, a non ser que dependa exclusivamente do consentimento da persoa interesada.
5. Na solicitude de cancelación, a persoa interesada debe indicar se revoga o consentimento outorgado, de ser o caso, ou se pretende a cancelación dun dato erróneo ou inexacto, para o cal deberá acompañar a documentación xustificativa.
6. O responsable do tratamento deberá facer efectiva a rectificación ou cancelación, cando proceda, no prazo de dez días.
7. A rectificación ou cancelación poderá denegarse motivadamente cando concorran razóns de interese público ou para salvagardar dereitos ou intereses de terceiros máis dignos de protección. O afectado a quen se lle denegan estes dereitos poderá poñelo en coñecemento do director da Axenda de Protección de Datos, que decidirá sobre a procedencia ou improcedencia da denegación.

9. Dereito de oposición

As persoas afectadas polo tratamento de datos de carácter persoal nos casos nos que non sexa necesario o seu consentimento poderán opoñerse a ese tratamento, sempre que unha lei non dispoña o contrario, cando existan motivos fundados e lexítimos relativos a unha concreta situación persoal. Neste suposto, o responsable do ficheiro excluirá do tratamento os datos relativos á persoa afectada.

Disposición adicional

A USC disporá dun Documento de Seguridade de conformidade cos criterios que a continuación se recollen.

CRITERIOS DO DOCUMENTO DE SEGURIDADE

Consideracións normativas

No mes de outubro de 1995 a Unión Europea ditou a Directiva 95/46/CE do Parlamento Europeo e do Consello, de 24 de outubro de 1995, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos (Directiva de Protección de Datos), e máis tarde a Directiva 97/66/CE do Parlamento Europeo e do Consello, de 15 de decembro de 1997, relativa ao tratamento dos datos persoais e á protección da intimidade no sector das telecomunicacións.

No mes de decembro de 1999 procedeuse á transposición ao noso ordenamento da normativa comunitaria, por medio da vixente Lei Orgánica 15/1999, de 13 de decembro, de protección de datos de carácter persoal, BOE 14/12/1999, coñecida como LOPD, ditada co obxecto de garantir e protexer, no que concirne ao tratamento dos datos persoais, as liberdades públicas e os dereitos fundamentais das persoas físicas e, especialmente, da súa honra e intimidade persoal e familiar.

O Real Decreto 994/1999, do 11 de xuño, aprobou o Regulamento de medidas de seguridade dos ficheiros automatizados que conteñan datos de carácter persoal, e establece a obrigaón das organizacións de poñer en marcha diversas medidas destinadas a garantir a protección deses datos. Isto afecta a sistemas informáticos, arquivos de soportes de almacenamento, persoal, procedementos operativos, etc. O Regulamento dispón que “o responsable do ficheiro elaborará e implantará a normativa de seguridade mediante un documento de seguridade de obrigado cumprimento para o persoal con acceso aos datos automatizados de carácter persoal e aos sistemas de información”.

Pódese considerar o Documento de Seguridade como un macrodocumento configurado xuridicamente a modo de regulamento onde se regulan os sistemas e os medios de seguridade empregados polo responsable do ficheiro e dos datos co fin de garantir os dereitos dos afectados de acordo coas disposicións legais nacionais e comunitarias ao uso. O Documento de Seguridade é un regulamento interno de control que obriga e rexe para todos aqueles (persoas físicas ou xurídicas) que teñan acceso ás persoas e aos locais, ás máquinas, aos programas, ás instalacións ou ao mobiliario onde se tratan ou poden tratarse datos de carácter persoal, estendidos como calquera tipo de información que afecta directa ou indirectamente a persoas físicas identificadas ou identificables. Con este regulamento preténdese asegurar a confidencialidade e integridade da información, a intimidade persoal e o pleno exercicio dos dereitos persoais fronte á súa alteración, perda, tratamento ou acceso non autorizado.

O Documento de Seguridade está composto por dous elementos: un estático (Regulamento de medidas de seguridade) e outro dinámico (os rexistros perimetrais de uso, administración e autocontrol).

O Documento de Seguridade debe conter aínda que sexa nos seus aspectos mínimos:

- As políticas: medidas, normas, procedementos, regras e estándares; así como as funcións e obrigas do persoal.
- O Plan de Seguridade:
 - Ámbito de aplicación con detalle dos recursos protexidos.
 - Estrutura dos ficheiros e descrición dos sistemas.

- Procedemento de notificación, xestión e resposta ante as incidencias.
- Actuacións e adecuación legal.
- O Plan de Continxencia: procedementos de realización de copias de apoio e recuperación dos datos.
- Descrición detallada do sistema de información: arquitectura de rede, servidores, sistemas operativos e aplicacións.
- Ficheiros de carácter persoal e estrutura de datos, e tipos de datos e aplicacións que os utilizan.
- Responsabilidades dos usuarios do sistema, e organigrama e funcións respecto ao tratamento.

Ámbito de aplicación

O Documento de Seguridade da USC será de aplicación a todos os recursos protexidos da USC, entendendo como tales todos os sistemas de información empregados para o tratamento e almacenamento dos datos de carácter persoal desta Universidade. Os sistemas de información inclúen o conxunto de ficheiros automatizados e o seu contorno, o lugar onde se procesan os datos, o tipo de telecomunicación utilizada, os programas soportes e os equipos empregados para o almacenamento e tratamento dos datos de carácter persoal.

Xestión dos ficheiros de protección de datos de carácter persoal

As obrigas e funcións dos responsables de ficheiros de protección de datos de carácter persoal redactaranse segundo as instrucións e a terminoloxía empregada no R.D. 994/1999, de 11 de xuño.

O Consello de Goberno define a política de datos persoais e o reitor da USC execútaa asignando as correspondentes disposicións de creación, modificacións e baixa de ficheiros de datos persoais da USC. O responsable do ficheiro, dos datos e das súas aplicacións decide acerca da creación, usos e finalidades do ficheiro.

Os *responsables dos ficheiros* de datos persoais son os vicerreitores, o secretario xeral ou o xerente en función da natureza do ficheiro e da súa área de responsabilidade. Deben figurar nas correspondentes disposicións de creación de ficheiros de datos de carácter persoal.

O responsable do ficheiro ten as seguintes funcións:

- Autorizar expresamente o tratamento fóra dos locais nos que se sitúa o ficheiro (art. 6 do R.D. 994/99 Regulamento de Medidas de Seguridade).
- Autorizar o documento de seguridade (art. 8.1).
- Revisar e actualizar o documento de seguridade ante cambios nos sistemas de información ou na organización daqueles (art. 8.2).
- Adecuar o documento de seguridade á normativa vixente (art. 8.4).
- Adoptar as medidas necesarias para que o persoal coñeza as normas en materia de seguridade así como as consecuencias do seu incumprimento (art. 9).
- Manter unha relación dos usuarios do sistema cos seus dereitos de acceso autorizado (artigos 11.1, 12.1 e 12.3).
- Establecer os criterios para a definición dos dereitos de acceso dos usuarios (art. 12.4).

- Establecer mecanismos para evitar que os usuarios accedan a recursos con dereitos distintos aos autorizados (art. 12.2).
- Autorizar a saída de soportes fóra dos locais (art. 13).
- Verificar a definición e ampliación de procedementos de copia e recuperación (art. 14).
- Designar o responsable de seguridade, no seu caso (art. 16).
- Adoptar medidas correctoras de deficiencias detectadas en auditorías (art. 17).
- Implantar un mecanismo de identificación de usuarios e verificación de que está autorizado (art. 18).
- Autorizar por escrito a execución dos procesos de recuperación (art. 21).
- Ser o interlocutor que representa á USC ante a Axencia Española de Protección de Datos.

O responsable do ficheiro pode delegar as funcións de tratamento dos datos, esta delegación faise doada en institucións complexas estruturadas en grandes áreas funcionais.

Os *responsables do tratamento* dos ficheiros de datos persoais son os directores ou xefes de departamento, áreas ou servizos da USC onde se xestionan estes ficheiros. As súas funcións son:

- Controlar o cumprimento das medidas de seguridade aplicadas aos ficheiros con datos de carácter persoal automatizados polo sistema informático do seu servizo.
- Por encargo de responsable do ficheiro, asegurar que todos os usuarios dos sistemas do seu servizo ou departamento poidan aplicar os principios reflectidos neste documento.
- Por encargo do responsable do ficheiro concederá ou revogará os permisos de acceso aos datos de carácter persoal dos usuarios dos sistemas do seu servizo.

Exercerá como *responsable de seguridade* quen ocupe ese posto establecido na Relación de Postos de Traballo, e no seu defecto o Director da Área TIC ou a persoa que designe. Asígnase ao responsable de seguridade a función de coordinar e controlar as medidas de seguridade aplicables. Entre as súas funcións destacan:

- Coordinar aos encargados de seguridade de todos os ficheiros con datos de carácter persoal automatizados polos sistemas informáticos corporativos da USC.
- Por encargo do responsable dos ficheiros, asegurará que todo o persoal da Área TIC poida aplicar os principios reflectidos neste documento.
- Por encargo do responsable do ficheiro concederá ou revogará os permisos de administración e acceso aos ficheiros de datos de carácter persoal ao persoal da Área TIC.
- Analizar os informes de auditoría bianual elevando consideracións ao responsable do ficheiro (art.17.3).
- Realizar un control directo do rexistro de acceso, controlando que en ningún caso se desactiven os mecanismos que rexistran os accesos de usuarios a información clasificada no nivel de seguridade alto (art. 24.3).
- Revisará periodicamente información de control rexistrada e elaborará un informe das revisións realizadas e os problemas detectados polo menos unha vez ao mes (art. 24.5).

Os *encargados de seguridade* son aquelas persoas que teñen por función verificar o cumprimento da normativa de seguridade no tratamento dos datos no ámbito dos seus departamentos o das súas aplicacións.

Xunto co responsable do tratamento, responden só fronte ao responsable do ficheiro das garantías dos afectados polo tratamento ou a forma de tratamento dos datos, así coma da aplicación efectiva dos sistemas de seguridade.

Recaen sobre o *persoal de informática* todas as tarefas de xestión dos ficheiros de datos, sen que se requira o coñecemento do seu contido:

- Administrar os sistemas informáticos e desenvolver aplicacións de forma que permitan o acceso e o mantemento dos datos coas garantías de seguridade esixidas polo Regulamento.
- Administrar as bases de datos.
- Xestionar os contrasinais.
- Realizar copias de seguridade.
- Realizar calquera copia de datos, non permitidas ao resto de usuarios.
- Eliminación de soportes obsoletos.
- Manter rexistros de soportes, entrada/saída de soportes e incidencias.
- Proporcionar mecanismos que aseguren a unicidade, redundancia mínima, coherencia, integridade e seguridade dos datos comúns centralizados, compartidos por diferentes dependencias da USC, para facilitar así a aplicación de medidas de seguridade.

Creación, modificación e supresión dos ficheiros de datos de carácter persoal

1. A creación, modificación ou supresión dos ficheiros só poderá facerse mediante unha disposición xeral publicada no Diario Oficial de Galicia. No caso de supresión de ficheiros a disposición establecerá o seu destino ou as medidas adoptadas para a súa destrución. No caso de creación ou modificación a disposición terá que conter o seguinte:

- a finalidade do ficheiro e os usos previstos para aquel;
- as persoas ou colectivos sobre os que se pretenda obter datos de carácter persoal ou que resulten obrigados a proporcionarlos;
- o procedemento de recollida de datos de carácter persoal;
- a estrutura básica do ficheiro e a descrición dos tipos de datos de carácter persoal incluídos nel;
- as cesións de datos de carácter persoal a outras institucións públicas ou privadas e, no seu caso, as transferencias de datos que se teñan previsto a países terceiros;
- os órganos das administracións responsables do ficheiro;
- a posibilidade de acceso, rectificación, cancelación e oposición daqueles e, no seu caso, os servizos ou unidades ante os que puidesen exercitarse;
- as medidas de seguridade con indicación do nivel básico, medio ou alto esixible.

2. O procedemento de alta dun ficheiro consta de dúas fases: creación do ficheiro e envío á Área de Tecnoloxías da Información e das Comunicacions da información de creación do ficheiro para a súa implantación.

a) Creación do ficheiro.

O ficheiro será creado por parte do reitor da Universidade de Santiago de Compostela mediante a disposición correspondente. Esa creación de ficheiro só poderá facerse mediante disposición xeral publicada no BOE ou DOG. A creación dun ficheiro sen a autorización correspondente pode supoñer unha infracción grave.

b) Envío á Área de Tecnoloxías da Información e das Comunicacions da información de creación do ficheiro para a súa implantación.

A solicitude de alta envíase á Área TIC. Esta solicitude debe ir acompañada de:

- 1) Cuestionario para a recollida de datos para cubrir os impresos de notificación á Axencia Española de Protección de Datos (AEPD) do ficheiro, para a súa inscrición no Rexistro Xeral de Protección de Datos (RGPD) (se contivese información de carácter persoal). Estes impresos xestionanse e envíanse á AEPD desde a Área TIC.
- 2) Disposición pola que se crea o ficheiro.
- 3) En caso de ser xestionado pola Área TIC, requírase:
 - Os datos técnicos e administrativos necesarios para a súa posta en funcionamento, ou no seu defecto, a solicitude de estudo técnico para a posta en funcionamento daquel.
 - Aceptación por escrito do responsable do ficheiro dos procedementos de copias de apoio e recuperación de datos, así como a súa execución por parte dos administradores do sistema cando sexa necesario para garantir a continuidade do servizo mediante o formulario correspondente.
- 4) A Área TIC rexistrará ese ficheiro no seu inventario de bases de datos.

3. A modificación dun ficheiro correspóndelle ao reitor mediante a disposición pertinente, ao igual que na súa creación. A solicitude de modificación envíase á Área TIC, se esta foi designada como responsable de seguridade dese ficheiro no procedemento de creación do ficheiro ou en disposición correspondente. Esta solicitude debe ir acompañada de:

- 1) Cuestionario para a recollida de datos para cubrir os impresos de notificación á Axencia Española de Protección de Datos do ficheiro, para/con a súa inscrición no Rexistro de Protección de Datos (se contivese información nova de carácter persoal).
- 2) Disposición pola que se modifica o ficheiro.
- 3) En caso de ser xestionado pola Área TIC, esta require:
 - Os datos técnicos e administrativos necesarios para a súa posta en funcionamento.
 - Aceptación por escrito do responsable do ficheiro dos procedementos de copias de apoio e recuperación de datos, así como a súa execución por parte dos administradores do sistema cando sexa necesario para garantir a continuidade do servizo mediante o formulario correspondente.
- 4) A Área TIC rexistrará ese ficheiro no seu inventario de bases de datos.

4. A supresión de ficheiros só poderá facerse mediante disposición xeral publicada no Boletín Oficial do Estado ou no Diario Oficial de Galicia. Esta disposición conterà o destino daqueles ou, no seu caso, as previsións que se adopten para a súa destrución. A solicitude de baixa envíase á Área TIC e debe ir acompañada de:

- 1) Impresos de notificación á AEPD do ficheiro, para a súa supresión correspondente no RGPD se o ficheiro estivese rexistrado. Este envío e a xestión realízanse desde a Área TIC.
- 2) Disposición pola que se dá de baixa o ficheiro, nesta disposición deberase establecer o seu destino ou as medidas adoptadas para a súa destrución.

Unha vez recollida a baixa, a Área TIC procederá a:

- Realización das copias de seguridade.
- Baixa física e permanente dese ficheiro no sistema xestor de base de datos onde estea situado.
- Comunicación da baixa á Axencia Española de Protección de Datos.
- Actualización do rexistro de base de datos da Área TIC.

5. Realizaranse un mínimo de dúas copias de seguridade en dous formatos distintos do medio de produción. Estas copias gardaranse polo menos durante 5 anos. Posteriormente procederase á reutilización ou refugado dos ditos soportes, garantindo calquera recuperación indebida mediante a desmagnetización ou a regravación inmediata daqueles. A baixa deste ficheiro debe garantir o impedimento de calquera recuperación indebida, debe así existir un procedemento de borrado de soportes.

Protección

O responsable do ficheiro adoptará as medidas para que o persoal coñeza as normas de seguridade que afecten ao desenvolvemento das súas funcións así como as consecuencias en que puidera incurrir en caso de incumprimento.

O responsable do ficheiro designará un ou varios encargados de seguridade, que xunto ao responsable de seguridade serán os encargados de coordinar e controlar as medidas de seguridade definidas neste documento. Esta designación non supón a delegación de responsabilidade, que corresponde sempre ao responsable do ficheiro.

O responsable e os encargados de seguridade terán ben identificados e documentados aos usuarios do sistema e os tipos de acceso autorizados para eles.

Os usuarios coñecerán claramente cales son os niveis de protección de cada sistema e absteranse de utilizalo en forma diferente á prescrita, e noutro caso poderán incurrir en responsabilidade explícitas.

Os usuarios terán acceso autorizado unicamente a aqueles datos e recursos que precisen para o desenvolvemento das súas funcións. O responsable do ficheiro establecerá mecanismos para evitar que un usuario poida acceder a datos ou recursos con dereitos distintos dos autorizados.

Seguridade de acceso, procedemento de identificación e autenticación

O responsable de seguridade da Área TIC encargarse de manter e documentar os dereitos de acceso ao ficheiro de datos de cada usuario ou grupo de usuarios. Estes dereitos de acceso poden establecerse individualmente ou por grupo para perfís de usuarios segundo as funcións e postos de traballo daqueles.

Identificación

Para efectuar o seguimento das actividades de cada usuario no sistema, todos os usuarios dispoñen dun identificador único, o código de usuario, que este usa persoal e exclusivamente, asocia as actividades do sistema a un responsable individualizable.

O identificador non debe dar información acerca do privilexio no acceso ao sistema, como administrador, supervisor, etc.

Non se utilizarán identificadores compartidos ou multiusuario, xa que non permiten identificar univocamente á persoa que os utiliza.

O Servizo de Directorio da Universidade de Santiago de Compostela (SDUSC) permite a busca de usuarios da USC a partir de distintos datos destes, como identificador, nome, departamento, servizo, sistema de información e/ou aplicacións xunto cos seus privilexios, etc. En todo caso soamente se farán públicos aqueles datos que non sexan de carácter persoal (nome, apelidos, enderezo de correo, departamento ou servizo, etc.).

Relación de usuarios

O responsable e ou encargado de seguridade de cada ficheiro encargárase de manter actualizada a lista de usuarios e administradores xunto cos seus accesos autorizados, para todos os sistemas de información e ficheiros dependentes da Área TIC.

Autenticación

O mecanismo que se utiliza para autenticar que un identificador de usuario non é utilizado por outra persoa diferente ao seu propietario é o de contrasinal, ou clave secreta de cada usuario.

Cada un dos distintos usuarios dos sistemas de información unicamente poderá acceder aos recursos aos que o autorice o responsable ou encargado do seguridade.

Os contrasinais que a Área TIC estableza para os distintos sistemas de información deberán cambiarse coa periodicidade de 12 meses para os usuarios finais. Non se permitirá o cambio dese contrasinal durante polo menos unha semana, e almacenarase sempre de forma inintelixible mentres teñan vixencia. Debe establecerse (considerando que se poidan obviar puntos dependendo da criticidade dos recursos aos que se accede):

- Quen asigna os contrasinais, inicial e sucesivos, e modo e vías de distribución:
 - O primeiro contrasinal é asignado ao crearse un identificador de usuario (conta). O administrador debe indicar que o usuario deberá mudar o contrasinal no primeiro inicio de sesión que realice de tal forma que o administrador, que nun primeiro momento lle asigna o contrasinal, xa non o coñecerá.
 - O resto de contrasinais son modificados polo propio usuario final coa frecuencia que o obrigue o seu sistema de información. Este cambio debe conter un proceso de confirmación de contrasinais para evitar erros de tecleo.
- Lonxitude mínima.
 - A lonxitude mínima é de oito caracteres.

- Vixencia regular.
 - O contrasinal terá unha vixencia de 12 meses para os usuarios finais, non está permitido o cambio dese contrasinal durante polo menos unha semana.
- Bloqueos de contas.
 - Procederáse automaticamente a bloquear calquera conta de usuario cando se realicen cinco intentos errados de acceso.
 - De igual modo bloquearanse aquelas contas que durante un período de polo menos dous meses estean durmidas ou en estado de inactividade.
- Desbloqueo de contas.
 - Só mediante unha petición persoal se desbloqueará unha conta. Nos casos de esquecemento do contrasinal asignarase de novo outro contrasinal, o administrador debe indicar que o usuario deberá mudar o contrasinal no primeiro inicio de sesión que realice de tal forma que o administrador, que nun primeiro momento lle asigna o contrasinal, xa non o coñecerá.
 - O desbloqueo de contas deberá ser comunicado *a posteriori* (para dar máis axilidade) ao responsable ou encargado de seguridade, tanto se é por esquecemento do contrasinal coma se é por intentos fallados de acceso.
- Tempo de caducidade.
 - Avisarase ao usuario ao iniciar a sesión, cando o seu contrasinal vaia caducar en menos de 15 días, ofrecerásele así a posibilidade de cambio.

Funcións de todo o persoal con acceso a información de carácter persoal

Toda persoa tanto usuario final coma técnico administrador con acceso aos datos de carácter persoal e aos seus sistemas de información, ten a obrigação, na medida das súas posibilidades, de garantir a intimidade, integridade e confidencialidade da información que manexa. En particular deberá:

- Respetar o dereito de información na recollida de datos dos afectados polos ficheiros de datos de carácter persoal.
- Respetar en todo momento os dereitos de acceso, rectificación e cancelación dos afectados polos ficheiros de datos de carácter persoal.
- Non realizar copias non autorizadas de datos de carácter persoal.
- É obrigação de todo profesional contratado directa ou indirectamente pola USC gardar o segredo sobre todo aquilo que coñeza no exercicio das funcións para as que foi contratado. Esta restrición non só se aplica durante o tempo en que exista unha relación contractual, senón aínda despois de finalizar as súas relacións co titular do ficheiro ou o responsable de dito ficheiro.
- O persoal funcionario e laboral está obrigado tamén a gardar o segredo sobre as informacións que coñeza no exercicio das súas funcións, incluso despois de que cesen estas.
- Está prohibida a cesión dos identificadores e contrasinais. Cada identificador e contrasinal é de uso individual e será responsabilidade do usuario a utilización que se faga del.
- De igual modo, o usuario manterá a confidencialidade do contrasinal, non a escribirá en lugar non seguro.
- É obrigatorio informar ao responsable ou encargado de seguridade de calquera acceso non autorizado ou anomalía, ameaza, vulnerabilidade ou risco de seguridade observado ou cando se coñeza, o máis rapidamente posible. Non deberán nunca os

usuarios probar as súas sospeitas, xa que este labor lle correspondería ao responsable ou encargado de seguridade.

- Cando o posto de traballo quede desatendido durante un período de tempo significativo, deberanse cancelar as sesións activas *log-off* antes de irse e cerrar o equipo. Esta desconexión producírase cando se pechen todos os programas de forma adecuada. Se o período de tempo é curto terase que protexer o equipo cun bloqueado de teclado, pantalla, chave ou similar (protector de pantalla protexido por contrasinal).
- Os documentos e disquetes do usuario que conteñan datos de carácter persoal gardaranse baixo chave cando a oficina estea baleira ou non se requiran nese momento.
- A utilización da información do ficheiro farase de acordo aos fins para os cales foi creado.
- Dentro das posibilidades, o usuario manterán limpo de programas daniños o seu posto de traballo.
- Sempre que utilice ficheiros temporais creados a partir dos ficheiros aos cales teña acceso, manterá as medidas de seguridade adecuadas para garantir o acceso non autorizado a eles, eliminará o ficheiro temporal en canto termine de utilizalo.
- Non está permitida a saída do centro de traballo de soportes que conteñan ficheiros temporais a menos que estean rexistrados adecuadamente no rexistro de saída, debidamente autorizado.
- Os usuarios que manexen datos persoais procuraran manter o seu posto de traballo limpo de programas. A instalación de software que non sexa propiedade da USC ou da Intranet corporativa deberase poñer en coñecemento da Área TIC.
- Na xestión de procedementos administrativos utilizaranse exclusivamente os programas que facilita a USC. En ningún caso se poderá realizar nin encargar ningún programa para a xestión sen previo coñecemento da área TIC.
- É obrigatorio o cumprimento de toda normativa reflectidas no presente documento.

Medidas específicas para o nivel alto de seguridade

1. O nivel alto de seguridade é aplicable a datos de ideoloxía, relixión, crenzas, orixe racial, saúde ou vida sexual.

2. Todo acceso que se realice a calquera ficheiro con datos de nivel alto debe manter un rexistro de seguimento que almacene a seguinte información:

- Acceso aos sistemas de información:
 - Identificación única do usuario,
 - data/hora e
 - entrada autorizada ou denegada.
- Acceso á información especialmente protexida (rexistros de datos) dentro dos sistemas de información pasado o primeiro filtro:
 - Identificación única do usuario,
 - data/hora,
 - táboa do ficheiro especialmente protexida,
 - rexistro ao que se accede e
 - tipo de acceso (consulta, alta, baixa ou modificación).

Os mecanismos que permiten o funcionamento deste rexistro teñen que estar sempre activos para detectar posibles problemas para os ficheiros especialmente protexidos.

O contido deste rexistro conservarase por un tempo mínimo de dous anos. O responsable de seguridade elaborará un informe mensual das revisións efectuadas periodicamente e dos problemas detectados.

3. Ademais de cumprir con todo o especificado para o nivel medio, nas copias de apoio de nivel alto deberán respectar estes criterios:

- Os soportes que recollen as copias deberán ser destruídos totalmente, non se permitirá en ningún caso a reutilización do soporte para os datos de nivel alto, unha vez que finalice o seu ciclo de vida.
- Enviarase unha segunda copia a outro edificio ou sala que conte coas mesmas medidas de seguridade que a primeira (armario ignífugo de acceso restrinxido), e onde non poden afectarlle as mesmas incidencias.

4. A transmisión de datos a través de redes deberá realizarse cifrando os datos. Para evitar problemas de seguridade interna, sempre que sexa posible, e dependendo da criticidade dos datos, este cifrado realizarase extremo a extremo, desde o servidor ao cliente e viceversa.

Procedemento de notificación, xestión e resposta ante incidencias

Considérase “incidencia” calquera anomalía que afecte ou puidera afectar á seguridade dos datos. Cada vez que se detecte algunha anomalía (incidencias que afecten á confidencialidade, integridade, dispoñibilidade e autenticidade da información), que poida ser considerada como incidencia, esta notificarase inmediatamente ao responsable de seguridade e ao director da Área TIC.

O responsable de seguridade rexistrará e analizará esa incidencia e, xunto coas indicacións do director da Área TIC, poñerá en marcha as medidas necesarias para corrixir o problema, se isto é de índole técnica.

No caso de tratarse dun intento, errado ou non, de acceso a datos de persoal non autorizado, informarase ao usuario non autorizado (se é identificado) e, no seu caso, tomaranse as medidas disciplinarias pertinentes. No caso de que o intento de acceso sexa para persoal alleo á USC, porase en coñecemento da Secretaría Xeral para formular a denuncia correspondente.

Cando se detecte un fallo nos mecanismos de protección de datos, estes serán inmediatamente revisados para incrementar o seu nivel de protección.

Se fose necesaria unha recuperación de datos, estes restauraranse das copias de seguridade previa autorización por escrito (nivel medio de seguridade) do responsable do ficheiro e realizaranse manualmente as actualizacións necesarias para deixar a información no mesmo estado no que se atopaba antes da incidencia, sempre que sexa posible. Introducirase no rexistro de incidencias a información completa desa recuperación.

Manterase un rexistro das incidencias como ferramenta imprescindible para a prevención de posibles ataques á seguridade, así como para a persecución dos responsables daqueles. O rexistro dunha incidencia deberá constar polo menos dos seguintes datos:

- Referencia única

- Ficheiro afectado
- Equipo no que se atopa
- Tipo de incidencia (acceso, palabra clave, corrupción de arquivo, borrado accidental de información, etc.)
- Efectos derivados da incidencia
- Data
- Hora
- Quen a notifica
- A quen se notifica
- Proceso de recuperación

Controis periódicos do cumprimento do disposto no regulamento de seguridade e auditorías de seguridade

Os obxectivos destes controis son os seguintes:

- Determinar as deficiencias e debilidades dos controis existentes ou en fase de implantación
- Suxerir as medidas correctivas e preventivas para que esas deficiencias sexan eliminadas

Débase revisar se o inventario dos ficheiros especificados no documento de seguridade é completo, e se existen ficheiros que non foron incorporados, así como se o nivel de seguridade do ficheiro é o que se especifica no documento de seguridade.

Así mesmo, verificarase que o documento de seguridade (todo ou parte), incluíndo as funcións e obrigas do persoal, foi publicado ou divulgado entre o persoal con dereitos de acceso a datos de carácter persoal. Cada seis meses revisarase este documento e actualizarase dependendo das posibles modificacións da lexislación aplicable e da propia USC.

Tamén se auditarán os rexistros de accesos, incidencias, soportes, entrada e saída de soportes, permisos de usuarios, así como os “logs” dos sistemas buscando intentos de acceso indebidos. O responsable de seguridade elaborará un informe mensual do rexistro de accesos.

Cada dous anos realizarase unha auditoría interna (art. 17 R.D. 994/1999), máis polo miúdo, do cumprimento do disposto no regulamento, incluíndo servizos distintos do de informática. O persoal técnico da Área TIC prestará o apoio necesario para a obtención dos datos precisos para levar a cabo este traballo. O responsable de seguridade realizará un informe cos resultados desa auditoría que será revisado polo director da Área TIC, o que levará a cabo as medidas correctoras necesarias, se as houbera. Ese informe, así como as medidas correctoras, quedará a disposición da Axencia Española de Protección de Datos (AEPD) na Área TIC.

A auditoría informática abarca a revisión e avaliación de calquera aspecto dos sistemas automáticos de procesamento da información, incluíndo os procedementos non automatizados relacionados con eles e as interfaces correspondentes. A auditoría informática permite, mediante a análise e comprobación de aplicacións e/ou sistemas, redes, políticas e procedementos de seguridade, etc. detectar debilidades naqueles.