UNIVERSIDADE DA CORUÑA

RESOLUCIÓN REITORAL DO 22 DE XULLO DE 2019 POLA QUE SE APROBA A POLÍTICA DE SEGURIDADE DA INFORMACIÓN E PROTECCIÓN DE DATOS PERSOAIS NA UDC

1. Introdución

A información constitúe un activo estratéxico e imprescindible para conseguir os obxectivos e cumprir a misión que as leis e os Estatutos da Universidade da Coruña (UDC) determinan.

O desenvolvemento da administración electrónica, coa posta a disposición da comunidade universitaria, e da cidadanía en xeral, de cada vez máis servizos prestados por vía telemática, implica novos retos en materia de protección da información que se manexa.

A importancia destes servizos e a necesidade de asegurar a súa dispoñibilidade e o uso correcto recoñécese na Lei 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas.

Do mesmo modo, a Lei 40/2015, do 1 de outubro, do réxime xurídico do sector público, establece que a seguridade é un dos principios xerais que deberán respectar todas as administracións públicas na súa actuación e nas súas relacións recíprocas.

Para responder a estes requirimentos de seguridade, o Real decreto 951/2015, do 23 de outubro, de modificación do Real decreto 3/2010, do 8 de xaneiro, polo que se regula o esquema nacional de seguridade no ámbito da administración electrónica, establece que todos os órganos superiores das administracións públicas deberán dispor formalmente da súa política de seguridade, que conterá as directrices que rexerán a forma en que a organización deberá xestionar e protexer a información e os servizos electrónicos que presta.

Por outra banda, a UDC debe observar tamén os preceptos marcados no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016 (RXPD), relativo á protección das persoas físicas no que respecta ao tratamento de datos de carácter persoal e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (Regulamento xeral de protección de datos), así como a Lei orgánica 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais.

Por todo o exposto anteriormente, a UDC debe contar cunha Política de seguridade da información e protección de datos de carácter persoal.

2. Obxecto

O obxecto desta Política de seguridade da información e protección de datos persoais é o establecemento dun proceso de xestión, baseado na mellora continúa, que lle permita á UDC protexer axeitadamente a información que manexa, amosando, deste xeito, o seu compromiso cunha xestión dilixente e respectuosa cos dereitos dos usuarios na prestación dos seus servizos electrónicos.

3. Ámbito de aplicación

Esta política aplícase a toda a información creada, recibida ou utilizada nas actividades da universidade, incluíndo os datos persoais, así como aos medios de tratamento que se empreguen, independentemente de que sexan informatizados ou non.

O ámbito subxectivo será todo o persoal que utilice a información anteriormente referida ou os sistemas de información mediante os que se realiza o tratamento.

4. Obxectivos

Os obxectivos en materia de seguridade da información e protección de datos persoais da UDC serán asegurar a integridade, a dispoñibilidade, a autenticidade, a confidencialidade e a trazabilidade da informacións e os servizos utilizados en medios electrónicos que xestiona no exercicio das súas competencias, de xeito que:

- se cumpran os requisitos legais existentes no ámbito da seguridade da información e a protección dos datos persoais;
- se maximice o tempo de dispoñibilidade dos servizos prestados;
- se minimicen os incidentes de seguridade;
- se garantan os dereitos dos usuarios dos servizos;
- se racionalice o gasto en medidas de protección.

5. Principios

A actuación da UDC, no ámbito da seguridade da información, estará rexida polos seguintes principios:

- A seguridade da información é un proceso integral e incumbe a todos os membros da comunidade universitaria.
- A seguridade da información enténdese como un proceso de mellora continua.
- As medidas de seguridade estableceranse en función dos riscos a que estea sometida a información e os seus sistemas de tratamento.
- A seguridade da información incluirá as dimensión de integridade, dispoñibilidade, autenticidade, confidencialidade e trazabilidade e os aspectos de prevención, detección, resposta e recuperación.
- O acceso á información realizarase a través de mecanismos persoais e intransferibles e deberá ser debidamente autorizado.
- O nivel de acceso aos sistemas de información estará baseado nas necesidades do posto de traballo do usuario (principio de mínimo privilexio).
- Os sistemas deben deseñarse e configurarse de forma que garantan a seguridade por defecto.
- Os sistemas proporcionarán a mínima funcionalidade requirida para que presten o servizo para o que foron deseñados.
- As actuacións de tratamento de datos persoais levaranse a cabo respectando, adicionalmente, os seguintes principios:
    - Licitude, lealdade e transparencia.

- Limitación das finalidades para as que se solicitan os datos, de tal modo que sexan recollidos con fins determinados, explícitos e lexítimos, e non sexan tratados con fins incompatibles cos inicialmente previstos
- Minimización dos datos persoais, de forma que só se solicitarán os datos estritamente necesarios para as finalidades previstas.
- Exactitude, adoptaranse as medidas necesarias para corrixir os datos erróneos.
- Limitación do prazo de conservación, de maneira que a identificación das persoas interesadas non sexa permitida máis alá do tempo necesario para os fins de tratamento dos datos persoais
- A UDC adoptará as medidas que garantan o tratamento lícito dos datos persoais (responsabilidade proactiva).

6. Directrices na xestión da información

A UDC aplicará as seguintes directrices xerais no manexo da información. Estas directrices desenvolveranse mediante normativa detallada.

- A información e os servizos clasificaranse en niveis mediante criterios aprobados pola UDC. Esta categorización, xunto coas avaliacións de riscos que se realicen, modulará as medidas de seguridade que se deban aplicar.
- Os criterios anteriormente citados terán en conta a repercusión na capacidade da organización para lograr os seus obxectivos, a protección dos seus activos, o cumprimento das súas obrigas de prestación de servizos, o respecto á legalidade e os dereitos dos cidadáns.
- Estableceranse medidas de seguridade nas distintas capas que interveñen no tratamento da información. Estas medidas serán de natureza organizativa, física e lóxica.
- O persoal será formado e informado dos seus deberes e obrigas en materia de seguridade da información.
- As persoas con responsabilidade na operación ou administración de sistemas informáticos e de comunicacións recibirán formación específica para o seu manexo seguro.
- As persoas que traten información da UDC, que non teña o carácter de pública, teñen a obriga de manter a confidencialidade e sixilo, obriga que perdura despois de finalizar o vínculo coa universidade.
- Nas relacións con terceiras partes, provedores externos ou contratistas, incluiranse nos contratos ou convenios as cláusulas necesarias para que, no caso de que sexa necesario ou posible o acceso á información da UDC por parte de persoal externo, este se faga respectando o previsto nesta política e na súa normativa de desenvolvemento.
- Cando a UDC preste servizos a outros organismos, ou manexe información doutros organismos, estableceranse canles para o reporte e a coordinación para a reacción ante incidentes de seguridade.
- Disporase dun procedemento de xestión de incidentes de seguridade. Este rexistro empregarase para a mellora continua da seguridade do sistema.

- A UDC informará as persoas interesadas dos tratamentos de datos persoais que realice e garantirá e establecerá vías áxiles para o exercicio dos dereitos da persoa interesada en materia de protección de datos persoais: dereito de acceso, dereito de rectificación, dereito de supresión, dereito de limitación do tratamento, dereito de portabilidade, dereito de oposición e dereito de non ser obxecto de decisións individualizadas automatizadas, incluíndo a elaboración de perfís.

7. Obrigas e responsabilidades no manexo da información

7.1. Responsabilidades de todos os usuarios

Todas as persoas que utilicen a información da UDC ou os seus sistemas de tratamento teñen a obriga de coñecer e respectar o indicado nesta política e no marco normativo de desenvolvemento que a universidade aprobe.

De acordo co artigo 10 do Real decreto 3/2010, polo que se aproba o Esquema Nacional de Seguridade e do artigo 39 do Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, relativo á protección das persoas físicas no que respecta ao tratamento de datos de carácter persoal, na xestión da seguridade da información da UDC existirán os roles que se indican nos seguintes apartados.

7.2. Responsable da información e dos tratamentos

O responsable da información e dos tratamentos terá as seguintes funcións e responsabilidades:

- Determinar os requisitos de seguridade da información tratada.
- Determinar o uso e a finalidade dos datos persoais tratados.
- Velar pola inclusión das cláusulas informativas nos procesos de recollida de datos persoais.
- Velar pola inclusión das cláusulas relativas á seguridade e á confidencialidade nos contratos con terceiras partes.

A Universidade da Coruña será a responsable da información e de calquera tratamento de datos persoais que sexa realizado polo seu persoal no exercicio das súas funcións, para o que se designa especificamente como tal a Secretaría Xeral, sen prexuízo de que no Rexistro de actividades de tratamento se identifique o órgano, servizo ou unidade administrativa onde se leve a cabo unha determinada actividade de tratamento.

7.3. Responsables dos servizos

Os responsables dos servizos electrónicos, isto é, que se prestan mediante sistemas de información, terán as seguintes funcións e responsabilidades:

- Definir os requisitos de seguridade dos servizos electrónicos.
- Determinar o impacto dunha indispoñibilidade destes servizos nas actividades da UDC.

- Asegurarse da prestación dos servizos electrónicos da universidade e garantir que esta se realice en condicións óptimas de dispoñibilidade, accesibilidade e interoperabilidade.

A responsabilidade dos servizos electrónicos na UDC recaerá no reitor, salvo naqueles sistemas en que este nomee outra persoa.

7.4. Responsable dos sistemas

O responsable dos sistemas, que será nomeado polo reitor, terá as seguintes funcións e responsabilidades respecto da seguridade da información:

- Desenvolver, operar e manter os sistemas de información durante todo o seu ciclo de vida, incluíndo as súas especificacións, instalación e verificación do seu correcto funcionamento.
- Definir os criterios de uso e os servizos dispoñibles nos sistemas de información.
- Implantar as medidas de seguridade técnicas aprobadas nos plans de tratamento do risco.
- Colaborar no desenvolvemento da normativa de uso das tecnoloxías da información e comunicacións.
- Colaborar na redacción dos plans de continxencia, para o que se levarán a cabo as comprobacións necesarias para verificar a súa efectividade.

7.5. Delegado/a de protección de datos

As funcións e responsabilidades do/a delegado/a de protección de datos, tal e como indica o artigo 39 do RXPD, serán as seguintes:

- Informar e asesorar o responsable da información e do tratamento das obrigas que lles incumben de acordo co marco legal en protección de datos persoais.
- Supervisar o cumprimento do disposto na dita regulación, incluída a concienciación e formación do persoal que participa nos tratamentos.
- Ofrecer o asesoramento que se lle solicite acerca da avaliación de impacto relativa á protección de datos e supervisar a súa aplicación.
- Cooperar e actuar como punto de contacto da autoridade de control.

O/a delegado/a de protección de datos será nomeado/a polo reitor.

7.6. Responsable de seguridade da información

O responsable de seguridade, que será nomeado polo reitor, terá as seguintes funcións e responsabilidades:

- Determinar as decisións para satisfacer os requisitos de seguridade da información e dos servizos.
- Supervisar que as medidas de seguridade cumpran coas especificacións dadas polo responsable da información e os responsables dos servizos.

- Coordinar os exercicios de avaliación de riscos.
- Dirixir o desenvolvemento desta política e coordinar as accións necesarias para aprobar a normativa que para eses efectos sexa necesaria.
- Realizar ou promover as auditorías periódicas a que obriga o Esquema nacional de seguridade.
- Promover a formación e concienciación en materia de seguridade da información dentro do seu ámbito de responsabilidade.

O responsable de seguridade non deberá ter ningunha responsabilidade sobre a prestación dos servizos nin deberá estar baixo a dependencia xerárquica do responsable do sistema, e viceversa.

7.7. Responsable da seguridade física

A responsabilidade da seguridade física das instalacións correspóndelle a Xerencia.

8. Comité de Seguridade da Información

Co fin de garantir a correcta implantación da presente política e coordinar todas as accións que se deban realizar en materia de seguridade da información e protección de datos, a UDC creará un Comité de Seguridade da Información que terá as seguintes funcións:

- Promover a mellora continua da seguridade da información.
- Informar regularmente do estado da seguridade da información ao Consello de Goberno.
- Revisar esta política e propoñer as modificacións que sexan necesarias.
- Elaborar as normas de desenvolvemento desta política e propoñerlle a súa aprobación ao Consello de Goberno.
- Elaborar e aprobar guías, recomendacións e procedementos de seguridade da información.
- Coordinar as accións transversais en materia de seguridade da información
- Coordinar as avaliacións de riscos de cada un dos sistemas.
- Aprobar os plans de tratamento do risco e o risco residual.
- Promover a realización das auditorías periódicas que permitan verificar o cumprimento das obrigas da UDC en materia de seguridade.
- Promover actividades de formación e concienciación en materia de seguridade.
- Dirixir a política de comunicación das cuestións relacionadas coa seguridade da información.
- Resolver os conflitos de responsabilidades que poidan xurdir entre os diferentes responsables e remitirlle ao órgano competente aqueles casos en que non teña suficiente autoridade para decidir.

O Comité de Seguridade da Información estará composto polas seguintes persoas:

- o reitor, quen presidirá o Comité

- o secretario xeral
- o xerente
- a delegada de protección de datos
- os responsables dos servizos
- o responsable dos sistemas
- o responsable de seguridade da información
- unha persoa designada polo reitor

O Comité poderá incorporar ás súas reunións as persoas que considere oportunas en función dos asuntos que se traten.

9. Criterios para a xestión de riscos

A xestión dos riscos, proceso esencial en que basear as medidas de seguridade que se implanten, será obxecto de actualización permanente. Consistirá nunha fase de avaliación e noutra de tratamento dos riscos.

A avaliación dos riscos identificará as ameazas e vulnerabilidades que lles poidan afectar á información e aos servizos, e abarcará os principais factores internos e externos, tales como factores organizativos, tecnolóxicos, físicos, humanos e servizos de terceiros, entre outros.

O tratamento dos riscos consistirá na selección das medidas de seguridade necesarias, organizativas ou técnicas, para conseguir un risco residual aceptable pola organización, dentro dun contexto de equilibrio entre o esforzo na implantación das medidas de seguridade e o beneficio que estas proporcionen. O conxunto de medidas plasmaranse nun plan de tratamento do risco.

Os sistemas deberán ser obxecto dunha avaliación de riscos polo menos cada ano, cando cambie substancialmente a información manexada, cando cambien substancialmente os servizos prestados ou cando ocorra un incidente de seguridade grave ou se reporten vulnerabilidades graves que impliquen un cambio substancial nas salvagardas do sistema.

10. Desenvolvemento desta política

A presente política desenvolverase mediante un marco normativo completo co obxectivo de tratar todos aqueles aspectos específicos que o requiran, de xeito que as persoas que manexen a información coñezan as condicións que deben rexer o tratamento desta.

O marco normativo estruturarase en catro niveis:

- Primeiro nivel: política de seguridade da información e protección de datos persoais, que será aprobada mediante unha resolución reitoral.
- Segundo nivel: normas xerais de seguridade que emanen da política, que serán aprobadas polo Consello de Goberno.

- Terceiro nivel: procedementos de seguridade, que describirán como realizar unha actividade concreta.
- Cuarto nivel: recomendacións, guías, boas prácticas etc.

Correspóndelle ao Comité de Seguridade da Información aprobar os procedementos e os documentos do cuarto nivel.

A normativa aprobada porase a disposición de todas as persoas que a deban coñecer. A UDC promoverá accións formativas e de concienciación para a súa difusión e interpretación correctas.

11. Aprobación e entrada en vigor

A presente política entrará en vigor ao día seguinte da súa publicación no Taboleiro Electrónico Oficial da Universidade da Coruña.

Anexo I: glosario de termos

Ameaza: causa potencial dun incidente non desexado, que lles pode provocar danos a un sistema ou á organización.

Autenticidade: propiedade pola que unha persoa ou entidade é quen afirma ser.

Avaliación ou análise de riscos: proceso global de identificación e estimación dos riscos.

Categoría dun sistema: nivel, dentro da escala básica-media-alta, co que se adxectiva un sistema co obxecto de seleccionar as medidas de seguridades necesarias.

Confidencialidade: propiedade pola que a información non se pon a disposición ou se divulga a persoas, entidades ou procesos non autorizados.

Datos persoais: toda a información sobre unha persoa física identificada ou identificable.

Dispoñibilidade: propiedade da información ou dun servizo de ser accesible e utilizable por solicitude dunha entidade autorizada.

Incidente de seguridade: evento non desexado ou inesperado que ten unha probabilidade significativa de ameazar a seguridade da información e comprometer as operacións da organización.

Información: datos que teñen contido semántico (é dicir, significado) nun contexto determinado.

Integridade: propiedade da información relativa á súa exactitude e completude.

Medidas de seguridade: conxunto de disposicións encamiñadas a diminuír os riscos a que están sometidos a información e os sistemas de tratamento.

Risco: posibilidade de que unha ameaza concreta poida explotar unha vulnerabilidade para causar unha perda ou dano nun activo de información.

Risco residual: risco que permanece tras aplicar medidas de seguridade que figuran nos plans de tratamento do risco.

Servizo electrónico: función ou prestación desempeñada por algunha entidade, mediante sistemas de información electrónicos ou telemáticos, destinada a coidar intereses ou satisfacer necesidades da cidadanía.

Sistema de información: conxunto organizado de recursos para que a información se poida recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, poñer a disposición, presentar ou transmitir.

Tratamento do risco: proceso de modificación do risco mediante a implementación de medidas de seguridade.

Trazabilidade: calidade que permite que todas as accións realizadas sobre a información ou un sistema de tratamento poidan ser asociadas, de modo inequívoco, a un individuo ou a unha entidade.

Vulnerabilidade: debilidade dun compoñente dun sistema ou dunha medida de seguridade que pode ser aproveitada por unha ameaza e causar un incidente de seguridade.

Xestión de riscos: actividades coordinadas para dirixir e controlar unha organización con respecto ao risco. Componse da avaliación, ou análise, e do tratamento do risco.