Política de seguridade da información da USC

INTRODUCIÓN

A información é un activo estratéxico para a Universidade de Santiago de Compostela (USC), e debe ser adecuadamente protexida, sexa cal for a forma na que estea representada, almacenada ou sexa procesada.

Nesta contorna cabe destacar o papel das Tecnoloxías da Información e das Comunicacións (TIC) pola crecente importancia no tratamento desa información, sendo o rápido desenvolvemento destas tecnoloxías un dos factores principais que está a permitir que as Administracións Públicas melloren a súa eficiencia, posibilitando achegarse á cidadanía mediante novas canles de comunicación.

Pero a información e as tecnoloxías que a tratan están sometidas a riscos, internos e externos, que é necesario xestionar adecuadamente para situalos baixo limiares aceptables. Para iso, é necesario contar cun sistema de xestión da seguridade da información. Mediante esta ferramenta, os órganos de goberno da USC poderán establecer obxectivos e medir a efectividade das accións que, neste ámbito, leven a cabo. Esta necesidade está aliñada coa obrigatoriedade de cumprir co disposto no Real decreto 311/2023, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade (en diante, ENS). Estas normas definen precisamente un modelo de xestión da seguridade da información e serán, por tanto, a guía que seguirá a USC neste ámbito.

A seguridade da información ten como obxectivo reducir, ata un nivel aceptable, os riscos a que están sometidos a información, sistemas e servizos que dan apoio á actividade universitaria. Este nivel aceptable debe responder a unha valoración conxunta da gravidade das ameazas, os recursos dispoñibles, o respecto aos dereitos individuais e o cumprimento normativo.

Hai que ter presente que a seguridade da información precisa da colaboración e implicación de toda a comunidade universitaria, onde os órganos directivos, que aproban a presente política e son responsables da súa divulgación e implantación efectiva, ata as persoas usuarias finais dos sistemas de información. Por iso, toda a organización debe estar preparada para previr, detectar, reaccionar e recuperarse ante posibles incidentes de seguridade.

1. OBXECTO OU MISIÓN

A USC define a presente Política de Seguridade da Información, de carácter obrigatorio para toda a comunidade universitaria e empresas colaboradoras, tendo como obxectivo fundamental garantir a seguridade da información e a prestación continuada dos servizos que proporciona, actuando preventivamente, supervisando a actividade e reaccionando con presteza fronte aos incidentes que poidan ocorrer.

Esta política aplicarase a toda a información que se xere como consecuencia das actividades da Universidade, así como aos tratamentos dos que poida ser obxecto, independentemente que estes sexan manuais ou automatizados, e que inclúan ou non datos de carácter persoal.

Esta política debe sentar as bases para que o acceso, uso, custodia e salvagarda dos activos de información, dos que se serve a USC para desenvolver as súas funcións, realícense baixo garantías de seguridade, nas súas distintas dimensións:

- Integridade: propiedade ou característica consistente en que o activo de información non sexa alterado de maneira non autorizada.

- Dispoñibilidade: propiedade ou característica dos activos, consistente en que as entidades ou procesos autorizados teñan acceso aos mesmos cando o requiran.

- Confidencialidade: propiedade ou característica consistente en que a información nin se poña a disposición, nin se revele a persoas, entidades ou procesos non autorizados.

- Trazabilidade: propiedade ou característica consistente en que as actuacións dunha entidade poidan ser imputadas exclusivamente a dita entidade.

- Autenticidade: propiedade ou característica consistente en que unha entidade sexa quen di ser ou ben que garanta a fonte da que proceden os datos.

Baixo estas premisas os obxectivos específicos da Seguridade da Información na USC serán:

- Velar pola seguridade da información, nas distintas dimensións antes descritas.

- Xestionar formalmente a seguridade, en base a procesos de análises de riscos.

- Elaborar, manter e probar os plans de continxencias e continuidade da actividade que se definan para os distintos servizos ofrecidos pola USC.

- Realizar unha adecuada xestión de incidentes que afecten á seguridade da información.

- Manter informado a todo o persoal acerca dos requisitos de seguridade, e difundir boas prácticas no manexo da información.

- Proporcionar os niveis de seguridade acordados con terceiras partes cando se compartan ou cedan activos de información.

- Cumprir coa regulamentación e normativa vixente.

Esta Política de Seguridade:

- Aprobarase formalmente polo Consello de Goberno.

- Será revisada regularmente polo Comité de Seguridade da Información, de forma que se adapte ás novas circunstancias, técnicas ou organizativas, e evite a súa obsolescencia.

- Comunicarase a todas as persoas empregadas e ás empresas ou organismos externos que manexen información da USC.

2. MARCO NORMATIVO

O marco normativo das actividades da USC no ámbito desta Política de Seguridade da Información está integrado polas seguintes normas:

- Real Decreto 311/2023, de 3 de maio, polo que se regula o Esquema Nacional de Seguridade.

- Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, de 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (Regulamento xeral de protección de datos).

- Lei Orgánica 3/2018, de 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais.

- Lei 37/2007, de 16 de novembro, sobre reutilización da información do sector público.

- Real Decreto 4/2010, de 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperatividade no ámbito da Administración Electrónica.

- Lei 39/2015, de 1 de outubro, do procedemento administrativo común das administracións públicas.

- Lei 40/2015, de 1 de outubro, de réxime xurídico do sector público.

- Real Decreto Lexislativo 5/2015, de 30 de outubro, polo que se aproba o texto refundido da Lei do Estatuto Básico do Empregado Público.

- Real Decreto 1553/2005, de 23 de decembro, polo que se regula o documento nacional de identidade e os seus certificados de sinatura electrónica.

- Resolución de 13 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade de conformidade co Esquema Nacional de Seguridade.

- Lei 9/2017, de 8 de novembro, de Contratos do Sector Público, pola que se traspoñen ao ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23 /UE e 2014/24/UE, de 26 de febreiro de 2014.

- Real Decreto-lei 14/2019, de 31 de outubro, polo que se adoptan medidas urxentes por razóns de seguridade pública en materia de administración dixital, contratación do sector público e telecomunicacións.

- Resolución de 7 de outubro de 2016, da Secretaría de Estado de Administracións Públicas, pola que se aproba a Instrución Técnica de Seguridade de Informe do Estado da Seguridade.

- Resolución de 27 de marzo de 2018, da Secretaría de Estado de Función Pública, pola que se aproba a Instrución Técnica de Seguridade de Auditoría da Seguridade dos Sistemas de Información.

- Resolución de 13 de abril de 2018, da Secretaría de Estado de Función Pública, pola que se aproba a Instrución Técnica de Seguridade de Notificación de Incidentes de Seguridade.

Igualmente, deberanse ter en conta as posibles modificacións normativas e avances técnicos que poidan afectar o ámbito desta Política de Seguridade da Información.

3. ALCANCE

A Política de Seguridade da Información aplícase a toda a comunidade universitaria:persoal, alumnado, así como a empresas e organismos, sempre que traten información da USC.

Afecta a toda a información xerada, procesada e almacenada, independentemente do seu soporte e formato, utilizada en tarefas operativas ou administrativas; á información cedida dentro dun marco legal establecido, que será considerada como propia a efectos exclusivos da súa protección; a todos os sistemas utilizados para administrar e xestionar a información, sexan propios da USC ou alugados ou licenciados por ela.

4. PRINCIPIOS XERAIS

Alcance estratéxico.

- A seguridade da información debe contar co compromiso e apoio de todos os niveis directivos da Universidade, de forma que poida estar coordinada e integrada co resto das iniciativas estratéxicas da organización para conformar un todo coherente e eficaz.

Prevención, detección, resposta e conservación.

- A seguridade do sistema debe contemplar as accións relativas aos aspectos de prevención, detección e resposta, co obxecto de minimizar a súas vulnerabilidades e lograr que as ameazas sobre el non se materialicen ou que, cando suceda, non afecten gravemente á información que manexa ou aos servizos que presta.

- As medidas de prevención, que poderán incorporar compoñentes orientados á disuasión ou á redución da superficie de exposición, deben eliminar ou reducir a posibilidade de que las ameazas cheguen a materializarse.

- As medidas de detección irán dirixidas a descubrir a presenza dun ciberincidente.

- As medidas de resposta, que serán xestionadas en tempo oportuno, estarán orientadas á restauración da información e os servicios que puideran verse afectados por un incidente de seguridade.

- Sen diminución dos restantes principios básicos e requisitos mínimos establecidos, o sistema de información garantirá a conservación dos datos e información en soporte electrónico. Do mesmo xeito, o sistema manterá dispoñibles os servizos durante todo o ciclo vital da información dixital, a través dunha concepción e procedementos que sexan a base para a preservación dixital.

Existencia de liñas de defensa.

- O sistema de información disporá dunha estratexia de protección constituída por múltiples capas de seguridade, disposta de forma que, cando unha das capas sexa comprometida, permita: a) Desenvolver unha reacción adecuada fronte ós incidentes que non foi posible evitar, reducindo a probabilidade de que o sistema sexa comprometido no seu conxunto. b) Minimizar o impacto final sobre o sistema.

- As liñas de defensa estarán constituídas por medidas de natureza organizativa, física e lóxica.

Vixilancia continua e reevaluación periódica.

- A vixilancia continua permitirá a detección de actividades ou comportamentos anómalos e a súa oportuna resposta.

- A avaliación permanente do estado da seguridade dos activos permitirá medir a súa evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

- As medidas de seguridade se reevaluarán e actualizarán periodicamente, adecuando a súa eficacia á evolución dos riscos e os sistemas de protección, podendo chegar a reformular a seguridade, se fose necesario.

Diferenciación de responsabilidades.

- Nos sistemas de información se diferenciará a persoa responsable da información, a persoa responsable do servizo, a persoa responsable da seguridade e a persoa responsable do sistema.

- A responsabilidade da seguridade dos sistemas de información estará diferenciada da responsabilidade sobre a explotación dos sistemas de información concernidos.

A seguridade da información como proceso integral.

- A seguridade da información incumbe a todos os membros da organización.

- A seguridade enténdese como un proceso integral constituído por todos os elementos que posibilitan un sistema de información:técnicos, humanos, materiais e organizativos.

- A seguridade dos sistemas de información contemplará os aspectos de prevención, detección e corrección para conseguir que as ameazas sobre os mesmos non se materialicen ou non causen danos graves.

- Estableceranse medidas de seguridade nas distintas capas que interveñen no tratamento da información.

Xestión da seguridade baseada en riscos.

- A selección de medidas de seguridade realizarase en base á análise dos riscos aos que estea sometida a información e os seus sistemas de tratamento.

- Esta análise manterase permanentemente actualizada dentro dun ciclo de mellora continua.

- O establecemento de medidas de protección, detección e recuperación será proporcional aos potenciais riscos e á criticidade e valor da información e dos servizos afectados.

Mellora continua.

- A seguridade da información enténdese como un proceso de mellora continua.

- Periodicamente, a Universidade definirá un conxunto de obxectivos de seguridade que incluirán unha descrición de liñas de actuación previstas, os proxectos nos que se concretan, os obxectivos que se deben alcanzar e os indicadores de cumprimento e progreso correspondentes. Estes obxectivos, que tomarán en consideración os resultados das auditorías e da análise de risco, revisaranse anualmente.

- Se implantará un proceso que comportará, entre outras accións: a) Revisión da Política de Seguridade da Información. b) Revisión dos servizos e información e a súa categorización. c) Execución con periodicidade anual da análise de riscos. d) Realización de auditorías internas ou, cando procedan, externas. e) Revisión das medidas de seguridade. f) Revisión e actualización das normas e procedementos.

Autorización e control dos accesos.

- O acceso aos sistemas de información realizarase a través de mecanismos persoais e intransferibles e deberán ser debidamente autorizados.

- O nivel de acceso aos sistemas de información estará baseado nas necesidades do posto de traballo da persoa usuaria, aplicando o principio de mínimo privilexio.

Clasificación da información.

- Os activos de información que trata a Universidade deberán ser inventariados e clasificados en función da confidencialidade da mesma.

- Deberá designarse unha persoa responsable para cada activo de información.

- O nivel de protección e as medidas de seguridade que se deben aplicar aos devanditos activos terá en conta a súa clasificación.

Seguridade por defecto.

- Os sistemas deben deseñarse e configurarse de forma que garantan a seguridade por defecto.

- Os sistemas proporcionarán a mínima funcionalidade requirida para que a organización alcance os seus obxectivos.

Xestión de persoal.

- Todo o persoal deberá ser formado e informado dos seus deberes e obrigas en materia de seguridade da información.

- Todas as persoas usuarias dos sistemas de información son responsables da comprensión e cumprimento da Política de Seguridade da Información e das normas, procedementos, instrucións e recomendacións asociadas.

- O persoal que participe no tratamento de información ou teña acceso aos locais onde se custodie a información ou se realice o tratamento desta, terá que observar e facer observar as medidas de seguridade establecidas. Estas obrigas serán independentes do tipo de relación xurídica que se manteña coa Universidade.

- O significado e alcance do uso seguro da información e dos sistemas de tratamento poderase concretar en normas específicas.

- A información, independentemente do soporte en que se atope, así como os medios de tratamento da mesma, empregaranse para fins estritamente relacionados coas funcións profesionais e nunca para fins persoais ou distintos dos aprobados.

- Desenvolveranse a concienciación, capacitación e educación en materia de seguridade da información.

- Nas relacións con terceiras partes, provedores externos ou contratistas, as unidades responsables velarán para que se inclúan nos contratos ou convenios as cláusulas convenientes para que, no caso de que sexa necesario ou posible o acceso a información da Universidade por parte do persoal daquelas, este fágase respectando o previsto na política de seguridade da información da Universidade.

Función diferenciada.

- Evitaranse os riscos derivados dunha falta de segregación de funcións.

- Diferenciarase entre responsable da información, do servizo, dos sistemas de tratamento e de seguridade.

Rexistros de actividade.

Coa finalidade exclusiva de lograr o cumprimento da presente política, con plenas garantías do dereito á honra, á intimidade persoal e familiar e á propia imaxe das persoas afectadas, e de acordo coa normativa sobre protección de datos persoais, de función pública ou laboral, e demais disposicións que resulten de aplicación, rexistraranse as actividades das persoas usuarias, retendo a información necesaria para monitorizar, analizar, investigar e documentar actividades indebidas ou non autorizadas, permitindo identificar en cada momento a persoa que actúa.

Xestión de incidentes de seguridade.

- Disporase dun procedemento de xestión de incidentes de seguridade.

- Este procedemento cubrirá os mecanismos de detección, os criterios de clasificación, os procedementos de análise e resolución, así como as canles de comunicación ás partes interesadas e o rexistro das actuacións.

- Este rexistro empregarase para a mellora continua da seguridade do sistema.

Protección das instalacións.

- Os sistemas se instalarán en áreas separadas.

- Deseñarase un procedemento para cumprir con todas as medidas de seguridade físicas que protexan as instalacións.

- Será especialmente importante dividir en diferentes zonas todas as instalacións, prevendo lugares de acceso restrinxido, que deberán contar cun control de accesos ás mesmas.

- As instalacións, especialmente a sala do CPD, contarán con controis de temperatura e humidade, así como medidas contra lumes e inundacións, e garantía de subministro eléctrico.

Adquisición de produtos.

- Valoraranse positivamente aqueles que teñan certificada a funcionalidade de seguridade relacionada co obxecto da súa adquisición.

- O proceso de adquisición de produtos estará suxeito a protocolos, seguindo fielmente a lexislación aplicable ao Sector Público.

- Terase especial coidado con que os novos compoñentes do sistema de información non afecten a outros xa existentes, ademais de confirmar que os novos compoñentes son congruentes coas distintas capacidades do sistema.

Integridade e actualización do sistema.

- Todo elemento físico ou lóxico requirirá autorización formal previa á súa instalación no sistema.

- Se deberá coñecer en todo momento o estado de seguridade dos sistemas, en relación ás especificacións dos fabricantes, ás vulnerabilidades e ás actualizacións que lles afecten, reaccionando con dilixencia para xestionar o risco á vista do estado de seguridade dos mesmos.

Prevención ante outros sistemas de información interconectados.

- O sistema debe protexer o perímetro, en particular, se está conectado a redes públicas. En todo caso se analizarán os riscos derivados da interconexión do sistema, a través de redes, con outros sistemas e se controlará o seu punto de unión.

Continuidade da actividade.

- Os sistemas disporán de copias de seguridade, establecéndose os mecanismos necesarios para garantir a continuidade das operacións, en caso de perda dos medios habituais de traballo.

Os principios xerais, anteriormente descritos, poderán ser desenvolvidos mediante normativa específica.

5. ORGANIZACIÓN DE SEGURIDADE

Co fin de garantir a correcta implantación da presente Política, a USC organizarase co obxecto de definir as medidas de seguridade que deben aplicarse aos activos de información.

Dita organización da seguridade conta coa participación activa dos órganos de goberno da USC, que aprobarán a Política de Seguridade da Información e asignarán ou delegarán responsabilidades nas persoas que consideren idóneas, e periodicamente, serán informados para asegurar o seguimento da implantación efectiva da mesma.

Así pois, os órganos de goberno da entidade cobran unha importancia capital:asumen o compromiso da entidade coa seguridade e a súa axeitada implantación, xestión e mantemento.

Igualmente, a organización implicará en distinta medida a todo o persoal da USC, co obxecto de estender a implantación das prácticas de seguridade idóneas.

A USC poderá crear un sistema de xestión da seguridade da información.

5.1. Estrutura organizativa: Funcións e responsabilidades

Consello de Goberno.

Os órganos de goberno da USC aseguran o compromiso da Universidade na aplicación desta política de seguridade e do ENS aprobando as normas regulamentarias de desenvolvemento.

No ámbito de seguridade da información, o Consello de Goberno ten as seguintes funcións:

- Aprobar a presente Política de Seguridade da Información da USC e as súas posteriores modificacións a proposta do Comité de Seguridade da Información.

- Constituír e realizar o nomeamento das persoas integrantes do Comité de Seguridade da información.

- Aprobar os regulamentos ou disposicións de carácter xeral en materia de seguridade da información.

Comité de Seguridade da Información.

A Universidade contará cun Comité de Seguridade da Información, que terá a seguinte composición:

- Secretario/a Xeral ou persoa que designe, que o presidirá.

- Vicerreitor/a con competencias TIC, ou persoa que designe.

- Vicerreitor/a con competencias en investigación, ou persoa que designe.

- Xerente/a ou persoa que designe.

- Secretario/a Xeral Adxunto/a.

- Responsable do sistema, que é o Director/a da Área TIC.

- Responsable de Seguridade da Información, que exercerá a secretaría do Comité.

Cada órgano unipersoal designará os seus representantes e suplentes, para substituílo en caso de ausencia. Está designación farase constar no documento POSI-003-Membros do Comité de Seguridade da Información.

Ademais, o comité poderá propor a incorporación de ata dúas persoas do colectivo de PDI, pertencentes a departamentos ou áreas de coñecementos relacionados coa seguridade nos sistemas de información, co obxecto de que acheguen a súa experiencia e coñecementos ao comité, tanto no campo tecnolóxico como no campo legal. Tamén poderá convidar ás reunións ás persoas que considere relevantes en relación cos puntos da orde do día que se consideren, como invitados permanentes ou ocasionais.

As funcións do Comité de Seguridade da Información serán as seguintes:

- Promover a integración dos requisitos de seguridade cos obxectivos estratéxicos da USC.

- Asegurarse de que a Política de Seguridade teña en conta o marco legal vixente, incluíndo o referido á protección de datos de carácter persoal e á propiedade intelectual.

- Coordinar a implantación da Política de Seguridade da Información.

- Revisar a efectividade da Política de Seguridade da Información e mantela actualizada.

- Definir as pautas xerais en materia de seguridade da información a través da normativa desenvolvida.

- Publicar e difundir a normativa relativa á seguridade da información entre todas as persoas afectadas.

- Revisar os informes de incidentes de seguridade máis significativos.

- Controlar as ameazas sobre a información e outros activos.

- Investigar e actuar para previr incidentes de seguridade.

- Definir roles e responsabilidades das distintas funcións relacionadas coa seguridade da información.

- Promover o desenvolvemento de iniciativas destinadas a melloras da seguridade.

- Definir as accións a seguir no caso de situacións non previstas, en relación á seguridade da información ou ante casos de incumprimento da normativa.

- Manter informado ó equipo de alta dirección da USC das iniciativas relevantes en materia de seguridade promovidas na USC.

- Elaborar instrucións, guías, modelos-tipo etc., para o mellor funcionamento da USC en materia de seguridade da información.

- Resolver os conflitos que podan aparecer entre as diferentes persoas responsables, elevando aqueles casos non que non teña suficiente autoridade para decidir.

Oficina de Seguridade da Información.

A Universidade contará cunha Oficina de Seguridade da Información, que terá a seguinte composición:

- O/A Director/a da Oficina de Seguridade de la Información, nomeado polo Comité de Seguridade da Información, que actuará como enlace entrambos, que será a persoa Responsable de Seguridade (RSEG), ou en quen delegue.

- Secretario/a da Oficina de Seguridade da Información, nomeado polo Comité de Seguridade da Información.

- Os/As Administradores Especialistas de Seguridade que a persoa Responsable de Seguridade da Información considere necesario.

As funcións da Oficina de Seguridade da Información serán, entre outras que lle poidan ser encomendadas polo Comité de Seguridade da Información:

- Xestión e operativa da seguridade do Proxecto de Adecuación, Implantación e xestión da Conformidade no ENS, análise e xestión de riscos, explotación, normativa e mantemento.

- Redacción e presentación de propostas ao Comité de Seguridade da Información. Elaborará os aspectos relacionados coa ciberseguridade e debaterá sobre eles en primeira instancia, para ser trasladados ao Comité.

- Promover a mellora continua do sistema de xestión da Seguridade da Información.

Centro de Operacións de Ciberseguridade.

As funcións que se atribúen ao Centro de Operacións de Ciberseguridade serán asumidas pola Área TIC da organización.

5. 2. Roles: Funcións e responsabilidades.

A continuación, cítanse os roles implicados na organización da seguridade da información na USC.

Responsable da información.

A figura de responsable da información recaerá na Secretaría Xeral.

A persoa responsable da información terá as seguintes funcións e responsabilidades:

- Determinar os requisitos de seguridade da información tratada, necesarios para protexer apropiadamente a información das aplicacións, e concretar os intereses a salvagardar, así como as necesidades a cubrir.

- Definir, para a información baixo a súa responsabilidade, as dimensións da seguridade relevantes (dispoñibilidade, confidencialidade, integridade, autenticidade e trazabilidade) e o seu nivel correspondente.

- Velar pola inclusión de cláusulas sobre seguridade nos contratos con terceiras partes ou polo seu cumprimento.

- Determinar a clasificación da categoría do sistema e as medidas de seguridade que deben aplicarse na Universidade.

- Calquera outra función que poida ser encomendada polos órganos correspondentes.

Responsable dos servizos.

A responsabilidade de primeiro nivel sobre os servizos do Sistema Xeral de Seguridade da Información recae sobre a persoa titular da Xerencia, membro nato do Comité de Seguridade da Información. As persoas responsables de cada servizo poderán participar nas reunións do comité cando se considere oportuno ou algún dos temas tratados afecten aos seus servizos.

As persoas responsables dos distintos servizos ou unidades administrativas terán as seguintes funcións e responsabilidades:

- Definir as necesidades de seguridade dos servizos contemplados na análise de riscos nas diferentes dimensións de seguridade (dispoñibilidade, confidencialidade, integridade, autenticidade e trazabilidade) e o seu nivel correspondente.

- Determinar para os servizos electrónicos baixo a súa responsabilidade a evolución do impacto dunha indispoñibilidade en función do tempo.

- Colaborar na análise de impacto dos incidentes que se poidan producir e expor as estratexias e salvagardas ante eles.

- Determinar, xunto coas persoas responsables da información, a clasificación da categoría do sistema e as medidas de seguridade que deben aplicarse na Universidade.

- Dar conta dos incidentes de seguridade dos que teñan coñecemento.

- Calquera outra función que se entenda pertinente no ámbito das funcións xerais que lles corresponden.

A Universidade, a través do Comité de Seguridade da Información, manterá unha relación das persoas responsables dos servizos afectados pola aplicación da política de seguridade da información.

Responsable de seguridade da información.

A figura de responsable de seguridade da información recaerá na persoa que exerza o posto dentro do organigrama da Secretaría Xeral e non poderá coincidir con ningún outro rol dos que figuran no presente documento.

Ademais de formar parte do Comité de Seguridade da Información, a persoa responsable de seguridade da información terá as seguintes funcións e responsabilidades específicas:

- Asegurar a definición de metodoloxías e procesos de seguridade homoxéneos en toda a USC.

- Inventariar a clasificación da categoría dos sistemas e as medidas de seguridade que deben aplicarse na Universidade.

- Coordinar as tarefas periódicas derivadas da revisión e mantemento da Análise de Riscos e da Análise de Impacto definido na Universidade.

- Reportar o estado da seguridade ao Comité de Seguridade da Información.

- Impulsar ou instar xunto co Comité de Seguridade da Información a realización de auditorías periódicas que permitan verificar o cumprimento das obrigas en materia de seguridade.

- Controlar os incidentes de seguridade e coordinar as accións correctoras pertinentes.

- Colaborar co resto do persoal técnico no desenvolvemento das iniciativas de seguridade.

- Asesorar ás distintas unidades técnicas na definición e implantación de procedementos e de medidas técnicas de seguridade.

- Promover na USC as medidas de concienciación necesarias en materia de seguridade da información.

Para determinados Sistemas de Información que, pola súa complexidade, distribución, separación física dos seus elementos ou número de usuarios, precisen de persoal adicional para levar a cabo as funcións do responsable da seguridade, poderán designarse responsables de seguridade delegados ou subresponsables. A designación será realizada pola persoa responsable de seguridade e concretará as funcións que se lles delegan. Non obstante o anterior, a responsabilidade final seguirá recaendo na persoa delegante.

Responsable dos sistemas.

A figura de responsable dos sistemas recaerá na persoa responsable da Área de Tecnoloxías da Información e das Comunicacións da USC, membro nato do Comité de Seguridade da Información, que poderá designar como persoas responsables do sistema delegadas a cada unha das persoas responsables técnicas da devandita área relacionados cos sistemas identificados no alcance do ENS; non obstante, a responsabilidade final seguirá recaendo na persoa delegante.

A persoa responsable dos sistemas ten as seguintes funcións e responsabilidades:

- Garantir que as tarefas propias da administración da seguridade dos sistemas baixo a súa responsabilidade lévanse a cabo de maneira correcta.

- Garantir que os sistemas de información dos que é responsable permanecen baixo control.

- Levar a cabo os procesos de seguridade no ámbito da súa área.

- Implementar a seguridade física e lóxica da Universidade.

- Colaborar nas auditorías de seguridade, LOPD e na xestión de riscos.

- Calquera outra función que se entenda pertinente no ámbito das funcións xerais que lles corresponden.

Serán invitadas permanentes ás reunións do Comité de Seguridade da Información as persoas responsables das áreas de sistemas e de seguridade dentro da ATIC.

Organización da protección de datos.

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

O Rexistro de Actividades de Tratamento detalla os arquivos afectados e as persoas responsables correspondentes, así como as medidas adoptadas neste marco. Todos os niveles de seguridade dos sistemas de información se replicarán nos tratamentos de datos persoais requiridos, segundo a súa natureza e finalidade.

Nesta materia xorden varias responsabilidades a nivel legal ou organizativo.

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

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

c) Persoa Delegada 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:

- Terá que ser unha persoa profesional que poida acreditar formación e coñecementos especializados en materia de protección de datos.

- Deberá 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 á seguridade da información.

- Poderá establecerse a través de contratación externa ou mediante designación dentro do cadro de persoal da organización.

- Será interlocutor necesario coa Autoridade de Control da Protección de Datos.

- Informará e asesorará á persoa responsable e/ou á persoa encargada do tratamento e ás persoas empregadas 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 dos Estados membros.

- Supervisará o cumprimento tanto do disposto no Regulamento e noutras disposicións de protección de datos da Unión ou dos Estados membros como das políticas do responsable ou do encargado do tratamento en materia de protección de datos persoais, incluída a asignación de responsabilidades, a concienciación e a formación do persoal que participa nas operacións de tratamento.

- Supervisará a realización das auditorías correspondentes.

- Ofrecerá o asesoramento que se lle pida acerca da avaliación de impacto relativa á protección de datos e supervisará a súa realización.

- Cooperará e actuará en contacto coa autoridade de control, neste caso a Agencia de Protección de Datos, para as cuestións relacionadas co tratamento de datos persoais, incluída a consulta previa e calquera outro tipo de consulta.

Integrada dentro da Política de Seguridade, terá as seguintes funcións e prerrogativas:

- Ser oída en todos os aspectos relacionados coa seguridade dos datos persoais e violacións de seguridade de datos persoais, entendendo as mesmas desde a perspectiva da confidencialidade, integridade e dispoñibilidade.

- Participar, como invitada permanente, nas reunións do Comité de Seguridade.

- Emitir o seu parecer naqueles aspectos relacionados coa seguridade dos datos persoais, promover, no seu caso, revisións de análise de riscos, elaboración de avaliacións de impacto

en protección de datos, elaboración ou modificación de procedementos ou políticas de seguridade de datos persoais, entre outros.

- Promover accións de formación e concienciación en privacidade.

- En xeral, todas as que teñan que ver coa protección de datos na entidade.

d) Secretaría Xeral:corresponde a este órgano a implementación da política de protección de datos e a xestión dos seus procedementos.

5.3. Xerarquía no proceso de decisións.

Os diferentes roles de seguridade da información (autoridade principal e posibles delegadas) se limitan a unha xerarquía simple:

1.- O Consello de Goberno aproba a normativa en materia de seguridade.

2.- O Comité de Seguridade da Información aproba as instrucións e guías que desenvolven a normativa, marcando directrices á persoa responsable de seguridade.

3.- A persoa responsable de seguridade da información executa a normativa, as instrucións e guías, supervisando que se implementen as medidas de seguridade segundo o establecido na política de seguridade aprobada.

Ademais, informa:

a) á persoa responsable da información sobre as decisións e incidentes en materia de seguridade que afecten á información que lle compete, en particular da estimación de risco residual e das desviacións significativas de risco respecto das marxes aprobadas.

b) á persoa responsable do servizo sobre as decisións e incidentes en materia de seguridade que afecten ao servizo que lle compete, en particular da estimación de risco residual e das desviacións significativas de risco respecto das marxes aprobadas.

c) ao Comité de Seguridade, reportando como secretaria:

resumo consolidado de actuacións en materia de seguridade

resumo consolidado de incidentes relativos á seguridade da información

estado da seguridade do sistema, en particular do risco residual ao que o sistema está exposto

4.- A persoa responsable do sistema informa á persoa responsable de seguridade da información:

- das incidencias funcionais relativas á información que lle compete.

- das accións de configuración, actualización ou corrección.

- dos incidentes de seguridade dos que teñan coñecemento.

Tamén informa á persoa responsable do servizo das incidencias funcionais relativas ao servizo que lle compete.

Por outra parte, reportan á persoa responsable da seguridade as actuacións en materia de seguridade; en particular no relativo a decisións de:

- arquitectura do sistema

- resumo consolidado dos incidentes de seguridade

- métricas da eficacia das medidas de protección que se deben implantar

Procedementos de designación de persoas

A USC, mediante o sistema legalmente establecido, nomeará formalmente:

- ao órgano responsable da información; que será a Secretaría Xeral da USC

- á persoa responsable do servizo; que será o responsable das unidades administrativas nomeadas conforme á normativa aplicable.

- á persoa responsable da seguridade da información, que debe reportar directamente ao Comité de Seguridade da Información e á Dirección.

- á persoa responsable dos sistemas, conforme á normativa aplicable.

Procedementos para resolución de conflitos e coordinación entre as persoas responsables En caso de confli to, prevalecerán as decisións do nivel superior xerárquico, que atenden á orde exposta no apartado anterior de xerarquía.

Para a coordinación e implantación da Política de Seguridade, o Comité de Seguridade da Información será o órgano competente onde deberán resolverse todas as cuestións de coordinación e resolución de conflitos que xurdan en materia de seguridade da información.

6. XESTIÓN DE RISCOS

Xustificación.

Todos os sistemas suxeitos a esta Política deberán realizar unha análise de riscos, avaliando as ameazas e os riscos aos que están expostos.

A análise de riscos será a base para determinar as medidas de seguridade que se deben adoptar, ademais dos mínimos establecidos polo Esquema Nacional de Seguridade, segundo lo previsto no Artigo 6 do ENS.

Criterios de avaliación de riscos.

Para a harmonización das análises de riscos, o Comité de Seguridade da Información establecerá unha valoración de referencia para os diferentes tipos de información manexados e os diferentes servizos prestados.

Os criterios de avaliación de riscos detallados se especificarán na metodoloxía de avaliación de riscos que elaborará a organización, baseándose en estándares e boas prácticas recoñecidas.

Deberán tratarse, como mínimo, todos os riscos que poidan impedir a prestación dos servizos ou o cumprimento da misión da organización de forma grave.

Daráselle prioridade especialmente aos riscos que impliquen un cese na prestación de servizos aos cidadáns.

A xestión de riscos atenderá ás necesidades de protección dos datos de carácter persoal, conforme require o artigo 32 do RGPD, motivo polo que incluíronse as actividades de tratamento.

Directrices de tratamento.

O Comité de Seguridade da Información dinamizará a dispoñibilidade de recursos para atender ás necesidades de seguridade dos diferentes sistemas, promovendo inversións de carácter horizontal.

Proceso de aceptación do risco residual.

Os riscos residuais serán determinados pola persoa Responsable de Seguridade da Información.

Os niveles de risco residuais esperados sobre cada Información trala implementación das opcións de tratamento previstas (incluída a implantación das medidas de seguridade previstas no Anexo II do ENS) deberán ser aceptados previamente pola persoa responsable desa Información.

Os niveles de risco residuais esperados sobre cada Servizo trala implementación das opcións de tratamento previstas (incluída a implantación das medidas de seguridade previstas no Anexo II do ENS) deberán ser aceptados previamente pola persoa responsable dese Servizo.

Os niveles de risco residuais serán presentados pola persoa responsable de seguridade ao Comité de Seguridade da Información, para que este proceda, no seu caso, a avaliar, aprobar ou rectificar as opcións de tratamento propostas.

A persoa DPD poderá ser escoitada no que respecta aos riscos en materia de protección de datos persoais.

Necesidade de realizar ou actualizar as avaliacións de riscos.

A análise dos riscos e o seu tratamento deben ser unha actividade repetida regularmente, segundo o establecido no Artigo 9 do ENS. Esta análise se repetirá:

- regularmente, cando menos unha vez ao ano.

- cando se produzan cambios significativos na información manexada.

- cando se produzan cambios significativos nos servizos prestados.

- cando se produzan cambios significativos nos sistemas que tratan a información e interveñen na prestación dos servizos.

- cando ocorra un incidente grave de seguridade.

- cando se reporten vulnerabilidades graves.

7. RELACIÓN CON PROTECCIÓN DE DATOS PERSOAIS

En materia de protección de datos, a entidade, seguindo a mesma liña que a exposta ata o momento, actuará baixo os seguintes principios adicionais:

- Licitude, lealdade e transparencia:os datos de carácter persoal serán tratados de maneira lícita, leal e transparente en relación co interesado.

- Lexitimación no tratamento de datos persoais:só se tratarán os datos de carácter persoal cando o tratamento se atope amparado nalgunha das causas de lexitimación establecidas nos artigos 6 e 9 do RGPD.

- Limitación da finalidade:os datos de carácter persoal serán tratados para o cumprimento de fins determinados, explícitos e lexítimos, e no serán tratados ulteriormente de maneira incompatible cos devanditos fins.

- Minimización de datos:os datos de carácter persoal serán adecuados, pertinentes e limitados ao necesario en relación cos fins para os que son tratados.

- Exactitude: os datos de carácter persoal serán exactos e, si fora necesario, actualizados; se adoptarán todas as medidas razoables para que se supriman ou rectifiquen sen dilación os datos persoais que sexan inexactos con respecto aos fins para os que se tratan.

- Protección de datos e seguridade desde o deseño: a USC promoverá a implantación do principio de protección de datos desde o deseño co obxectivo de cumprir cos requisitos definidos no RGPD e, polo tanto, cos dereitos dos interesados de xeito que a protección de datos se atope presente nas primeiras fases da concepción de calquera tipo de proxecto ou sistema que implique un tratamento de datos persoais.

- Protección de datos por defecto: a USC promoverá que os sistemas de información da súa titularidade se deseñen e configuren de forma que garantan a protección de datos por defecto.

8. NORMATIVA DE SEGURIDADE DA INFORMACIÓN

A USC establece un marco documental estruturado en diferentes niveis, de forma que as directrices marcadas polo presente documento teñan un desenvolvemento específico. En calquera caso, as diferentes políticas, normativas e regulacións específicas que se desenvolvan deben estar aliñadas coa presente política de seguridade da información e derivarse da mesma.

A composición do citado marco documental é a seguinte:

- Política de Seguridade da Información: Está constituído polo presente documento e é de obrigado cumprimento.

- Normativas: Emanan da presente Política de Seguridade da Información e soportan os diferentes ámbitos da seguridade. Serán aprobadas polo Consello de Goberno da USC.

- Procedementos de seguridade: Emanan da presente Política de Seguridade da Información e soportan os diferentes ámbitos da seguridade. Serán aprobados polo Comité de Seguridade da Información.

- Guías específicas de TI ou instrucións técnicas: Conxunto de documentos que describen as pautas específicas a seguir á hora de realizar unha determinada actividade técnica relacionada coa seguridade da información. Serán aprobados polo Comité de Seguridade da Información ou polo órgano técnico que se designe.

- Outros documentos: Ademais dos documentos citados, a documentación de seguridade poderá contar con outros adicionais, como recomendacións, boas prácticas, informes, rexistros, evidencias electrónicas, presentacións, etc.

A Política de Seguridade da Información (primeiro nivel) e as normas de carácter xeral (segundo nivel) serán aprobadas polo Consello de Goberno da Universidade, a proposta do Comité de Seguridade da Información.

O seu incumprimento pode dar lugar á correspondente responsabilidade disciplinaria.

Os procedementos e guías de seguridade ou instrucións de seguridade (terceiro e cuarto nivel) son aprobadas polo Comité de Seguridade da Información a proposta da persoa responsable de Seguridade da Información en colaboración coas persoas responsables dos Servizos e dos Sistemas.

A presente Política de Seguridade da Información e as normativas que se aproben deben ser comunicadas a todas as persoas responsables dos servizos afectados, debendo estar publicadas no Taboleiro de Anuncios Electrónico Oficial da USC. O resto de documentación

específica deberá estar accesible na intranet da Universidade ou na páxina web pública, sempre que a súa aplicabilidade poida afectar a todas as persoas usuarias.

9. OBRIGAS ASOCIADAS

9.1 Obrigas xerais dos usuarios

Todas as persoas usuarias da Universidade teñen a obriga de coñecer e cumprir esta Política de Seguridade da Información e a normativa e instrucións de seguridade desenvolvidas a partir dela, sendo responsabilidade do Comité de Seguridade da Información dispor os medios necesarios para que a información chegue ás persoas afectadas.

Todas as persoas usuarias da Universidade deben ser conscientes da necesidade de garantir a seguridade dos sistemas de información, así como de que elas mesmas son unha peza esencial para o mantemento e mellora da seguridade.

Establecerase, a través dos programas de formación do persoal, actividades de concienciación continua para atender a todas as persoas usuarias da Universidade, en particular ás de nova incorporación. Todas as persoas con responsabilidade no uso, operación ou administración de sistemas TIC deberán recibir formación para o manexo seguro dos sistemas na medida en que a necesiten para realizar o seu traballo.

Todas as persoas usuarias da Universidade deben ser conscientes do que implica un incidente de seguridade e deberán notificalo coa maior brevidade desde a súa identificación ás oportuna persoas responsables. De conformidade co disposto no artigo 33 do RD 311 /2022, de 3 de maio, a Universidade notificará ao Centro Criptológico Nacional aqueles incidentes que teñan un impacto significativo na seguridade da información manexada e dos servizos prestados en relación coa categorización de sistemas recollida no Anexo I do Real Decreto.

9.2. Responsabilidades en caso de incumprimento

O Comité de Seguridade da Información poderá apreciar se por parte das persoas usuarias da Universidade podería existir algún tipo de incumprimento nas obrigas previstas na Política de Seguridade da Información ou na súa normativa e instrucións de desenvolvemento.

No caso de que se aprecie un posible incumprimento, adoptaranse medidas preventivas e correctoras encamiñadas a salvagardar e protexer a información e os medios de tratamento.

Igualmente, apreciado un posible incumprimento da Política de Seguridade da Información da Universidade, o Comité de Seguridade da Información poderá instar aos órganos correspondentes a instrución dos procedementos disciplinarios que se consideren convenientes.

O procedemento e as sancións que proceda aplicar serán as establecidas na lexislación estatal ou autonómica sobre réxime disciplinario do persoal ao servizo das Administracións Públicas.

10. TERCEIRAS PARTES

Cando a Universidade preste servizos a outros organismos o manexe información doutros organismos, se lles fará partícipes desta Política de Seguridade da Información. Se establecerán canles para o reporte e a coordinación dos respectivos Comités de Seguridade da Información e se establecerán procedementos de actuación para reaccionar ante incidentes de seguridade.

Cando a Universidade utilice servizos de terceiros ou ceda información a terceiros, se lles fará participes desta Política de Seguridade e da normativa de seguridade aplicable ao devanditos servizos ou información. A terceira parte quedará suxeita ás obrigas establecidas na normativa, podendo desenvolver os seus propios procedementos operativos para satisfacela. Se establecerán procedementos específicos de reporte e resolución de incidencias. Se garantirá que o persoal de terceiros está adecuadamente concienciado en materia de seguridade, cando menos ao mesmo nivel que o establecido nesta Política de Seguridade.

Cando algún aspecto desta Política de Seguridade da Información non poida ser satisfeito por unha terceira parte segundo se require nos parágrafos anteriores, se requirirá un informe da persoa Responsable de Seguridade que precise os riscos en que se incorre e o xeito de tratalos. Se requirirá a aprobación deste informe polos responsables da información e os servizos afectados antes de seguir adiante.

11. DERROGACIÓN, APROBACIÓN E ENTRADA EN VIGOR

Esta Política de Seguridade da Información derroga a aprobada con data de 24 de xullo de 2020.

Entrará en vigor na data de publicación no Taboleiro de Anuncios Electrónico da USC.

Esta Política terá plena validez e eficacia desde a súa entrada en vigor ata a súa substitución por unha nova.