III. OUTRAS DISPOSICIÓNS

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

RESOLUCIÓN do 4 de maio de 2018 pola que se lle dá publicidade á modificación da política de seguridade da información da Administración xeral e do sector público autonómico de Galicia.

O Decreto 73/2014, do 12 de xuño, polo que se crean e regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia establece que a Comisión de Seguridade e Goberno Electrónico proporá para a súa aprobación polo Consello da Xunta de Galicia a política de seguridade da Administración xeral e do sector público de Galicia. En consecuencia, tras a proposta que efectuou o Pleno da Comisión de Seguridade e Goberno Electrónico, o Consello da Xunta de Galicia, na súa reunión do día vinte e cinco de xuño de dous mil quince, acordou aprobar a política de seguridade da información da Administración xeral e do sector público autonómico de Galicia, que se publicou mediante Resolución da directora da Axencia para a Modernización Tecnolóxica de Galicia, do 10 de xullo de 2015 pola que se lle dá publicidade á política de seguridade da información da Administración xeral e do sector público autonómico de Galicia (DOG núm. 137, do 22 de xullo).

Desde a dita aprobación producíronse cambios na normativa vixente nesta área, entre os que destaca o Regulamento xeral de protección de datos, aprobado polo Parlamento Europeo e o Consello, que entrou en vigor o 25 de maio de 2016 e comezará a aplicarse o 25 de maio de 2018, polo que se fixo necesaria a revisión da política de seguridade da información da Administración xeral e do sector público autonómico de Galicia vixente ata agora. Así, tras o debate e elaboración dun novo texto no seo da Subcomisión de Seguridade, de acordo co previsto no Decreto 73/2014, do 12 de xuño, polo que se crean e regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia, o Pleno da Comisión de Seguridade e Goberno Electrónico na sesión ordinaria que tivo lugar o 11 de abril de 2018, acordou a proposta de elevación desta modificación ao Consello da Xunta, que a aprobou na súa reunión do día 19 de abril de 2018.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

Por todo o exposto,

RESOLVO:

Darlle publicidade á política de seguridade da información da Administración xeral e do sector público autonómico de Galicia, que se recolle no anexo que acompaña a esta resolución.

Santiago de Compostela, 4 de maio de 2018

Mar Pereira Álvarez
Directora da Axencia para a Modernización Tecnolóxica de Galicia

ANEXO

1. Política de seguridade da información da Administración xeral e do sector público autonómico de Galicia.

A misión da Xunta de Galicia céntrase en dirixir a política e a administración da Comunidade Autónoma de Galicia e en exercer a función executiva e a potestade regulamentaria, de acordo co Estatuto de autonomía e coas leis. A Administración xeral e o sector público autonómico de Galicia, baixo a dirección da Xunta de Galicia, atópanse inmersos nun proceso gradual de transición cara á sociedade da información e do coñecemento, o que comporta unha transformación substancial a nivel tecnolóxico.

Neste marco, as tecnoloxías da información e as comunicacións (TIC) constitúense como un instrumento de alto nivel estratéxico, debido ao seu potencial para impulsar a modernización da Administración xeral e do sector público autonómico de Galicia, así como á súa capacidade para estimular e sustentar o desenvolvemento social e económico de Galicia. Por tanto, é imprescindible que os sistemas TIC sexan administrados con dilixencia e tamén tomar as medidas adecuadas para protexelos de ameazas de rápida evolución e con potencial para incidir na confidencialidade, integridade, dispoñibilidade, rastrexabilidade, autenticidade e valor da información e dos servizos.

A política de seguridade da información é o instrumento en que se apoia a Administración xeral e o sector público autonómico de Galicia para alcanzar os seus obxectivos, utilizando de forma segura os sistemas de información e as comunicacións. Para defenderse das ameazas, garantir a continuidade dos sistemas de información, minimizar os riscos de dano e asegurar o eficiente cumprimento dos seus obxectivos, será necesario definir medidas de seguridade de natureza organizativa, física e lóxica. Todo iso permitirá reforzar

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

a seguridade para protexer cada activo, xa que a seguridade, concibida como proceso integral, comprende todos os elementos técnicos, humanos, materiais e organizativos relacionados cos sistemas de información e as comunicacións e debe entenderse non como un produto, senón como un continuo proceso de adaptación e mellora, que debe ser controlado e xestionado.

Por iso, esta política será de aplicación, en todo o ámbito da Administración xeral e o sector público autonómico de Galicia, a todos os seus recursos e á totalidade dos seus procesos, internos e externos, vinculados á Xunta de Galicia a través de contratos ou acordos con terceiros.

2. Marco normativo.

A presente política de seguridade desenvólvese no marco normativo establecido polas seguintes normas:

a) Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello do 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, en adiante, RXPD)

b) Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación dos ditos datos e pola que se derroga a Decisión Marco 2008/977/JAI do Consello.

c) Lei orgánica de protección de datos de carácter persoal e regulamento de desenvolvemento.

d) Real decreto 3/2010, do 8 de Xaneiro, polo que se regula o esquema nacional de seguridade no ámbito da Administración electrónica, modificado polo Real decreto 951/2015, do 23 de outubro (en adiante, ENS).

e) Decreto 230/2008, do 18 de setembro, polo que se establecen as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia (en adiante, Decreto boas prácticas)

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

f) Decreto 73/2014, do 12 de xuño, polo que se crean e se regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia, modificado polo Decreto 169/2016, do 24 de novembro (en adiante, Decreto 73/2014, do 12 de xuño).

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

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

3. Obxectivos e ámbito de aplicación.

3.1. Obxectivos da política de seguridade da información.

A política de seguridade da información da Administración xeral e do sector público autonómico de Galicia ten como obxectivo establecer os principios xerais que dirixen a xestión da seguridade no ámbito de aplicación do número 3.2. Persegue a protección dos recursos necesarios para alcanzar os obxectivos e a misión da organización, serve como declaración de intencións e guía xeral coa cal establecer todas as actuacións en materia de seguridade e fixa a estrutura que debe desenvolverse para acometer estas actuacións, tanto no ámbito organizativo como no documental.

A súa aprobación serve para constatar o interese de máximo nivel que suscita a protección da información manexada na Administración xeral e no sector público autonómico de Galicia e establece o punto de partida de organización para conseguir este fin.

A política de seguridade será revisada periodicamente polos órganos colexiados con responsabilidades en materia da seguridade da información e actualizada cando sexa necesario.

3.2. Ámbito de aplicación.

Esta política será de aplicación, no ámbito da Administración xeral e do sector público autonómico de Galicia, a todos os sistemas de tecnoloxías da información e comunicacións, infraestruturas e instalacións en xeral, e aos membros da súa organización, sen excepcións; tamén se aplicará no caso de entidades e profesionais contratados baixo calquera modalidade, cando no exercicio das súas funcións teñan acceso aos sistemas de tecnoloxías da información e comunicacións.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

4. Principios da política de seguridade da información.

A política de seguridade da información da Administración xeral e do sector público autonómico de Galicia desenvolverase, con carácter xeral, de acordo cos seguintes principios:

a) Principio de confidencialidade: deberase garantir que os activos sexan accesibles unicamente para aquelas persoas expresamente autorizadas para iso.

b) Principio de integridade: deberase asegurar que a información coa que se traballa sexa completa e precisa, e incidirase na exactitude tanto do seu contido como dos procesos involucrados.

c) Principio de dispoñibilidade, resiliencia e continuidade: garantirase a prestación continuada dos servizos e a recuperación inmediata ante posibles continxencias, mediante medidas de recuperación orientadas á restauración dos servizos e da información asociada. Débese procurar que os activos estean dispoñibles cando o requiran as persoas autorizadas para acceder a eles.

d) Principio de autenticidade: deberase garantir que a información se intercambie cos interlocutores idóneos e que os servizos se acrediten correctamente.

e) Principio de rastrexabilidade: deberase garantir o seguimento das operacións efectuadas sobre a información e os servizos que o requiran.

f) Principio de xestión do risco: xestionar a seguridade da información consiste en analizar os riscos, establecer medidas de seguridade adecuadas, eficaces e proporcionadas e incluír a corrección e a mellora continuas que leven a que a organización sexa cada vez máis preventiva ca reactiva fronte aos incidentes de seguridade. Débense minimizar os riscos ata niveis aceptables e buscar o equilibrio entre as medidas de seguridade e a natureza da información.

g) Principio de prevención: desenvolveranse plans e liñas de traballo específicas orientadas a previr fraudes, incumprimentos ou incidentes relacionados coa seguridade.

h) Principio de mellora continua: revisarase, de maneira recorrente, o grao de eficacia dos controis de seguridade implantados na organización para aumentar a capacidade de adaptación á constante evolución dos riscos e do ámbito tecnolóxico.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

i) Principio de proporcionalidade en custo: a implantación de medidas que mitiguen os riscos de seguridade dos activos deberá facerse dentro do marco orzamentario previsto para ese efecto e sempre buscando o equilibrio entre as medidas de seguridade, a natureza da información e o orzamento previsto.

j) Principio de concienciación e formación: articularanse programas de formación, sensibilización e concienciación para as persoas usuarias en materia de seguridade da información, debidamente apoiados nas políticas corporativas e cun acomodado proceso de seguimento e actualización.

k) Principio de seguridade no ciclo de vida: os requirimentos da seguridade da información atenderanse durante todo o ciclo de vida dos activos, desde a súa planificación ata a súa retirada, con especial atención a garantir a seguridade desde o deseño e por defecto.

l) Principio de función diferenciada: conforme o principio que establece o ENS de considerar a seguridade como unha función diferenciada, na Administración xeral e do sector público autonómico de Galicia a seguridade dos sistemas de información estará diferenciada da responsabilidade sobre a prestación dos servizos.

m) Principio de cumprimento normativo: todos os sistemas de información da Administración xeral e do sector público autonómico de Galicia, así como calquera proceso relacionado, axustaranse á normativa de aplicación legal regulamentaria e sectorial que afecte a seguridade da información, en especial aquela relacionada coa intimidade e a protección de datos de carácter persoal e coa seguridade dos sistemas, datos, comunicacións e servizos electrónicos, que lles permita aos cidadáns e ás administracións públicas o exercicio de dereitos e o cumprimento de deberes a través da tecnoloxía.

5. Organización da seguridade da información.

5.1. Responsabilidade xeral.

A preservación da seguridade da información será considerada obxectivo común de todas as persoas ao servizo da Administración xeral e do sector público autonómico de Galicia, e serán as persoas, xunto coa tecnoloxía e os procesos, o alicerce fundamental para o mantemento da seguridade da información.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

5.2. Comisión de Seguridade e Goberno Electrónico da Administración xeral e do sector público autonómico de Galicia.

A Comisión de Seguridade e Goberno Electrónico da Administración xeral e do sector público autonómico de Galicia ten como funcións as definidas no Decreto 73/2014, do 12 de xuño, polo que se crean e se regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia.

5.3. Subcomisión de Seguridade.

A Subcomisión de Seguridade ten como funcións as definidas no Decreto 73/2014, do 12 de xuño, polo que se crean e regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia.

5.4. Roles no ámbito da seguridade da información requiridos para o cumprimento do ENS.

Seguindo o principio que establece o ENS de considerar a seguridade como unha función diferenciada, nos distintos organismos da Administración xeral e do sector público autonómico de Galicia existirán o responsable da información, o responsable do servizo, o responsable da seguridade TIC e o responsable do sistema.

a) Responsable da información: dentro do seu ámbito de actuación, é o encargado de determinar as necesidades de seguridade da información no marco establecido polo anexo I do ENS e de aprobar o risco residual.

b) Responsable do servizo: dentro do seu ámbito de actuación, é o encargado de determinar as necesidades de seguridade do servizo no marco do anexo I do ENS, de aprobar a suspensión do servizo e de aprobar o risco residual.

c) Responsable da seguridade TIC: determinará as decisións tecnolóxicas, no ámbito dos sistemas de información e telecomunicacións, que se han tomar para protexer adecuadamente a información e os servizos segundo as necesidades establecidas polos responsables da información e dos servizos.

d) Responsable do sistema: dentro do seu ámbito de actuación, é o encargado de implantar e de controlar as medidas para cumprir cos requisitos de seguridade da información e dos servizos.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

5.5. Outros roles no ámbito da seguridade da información.

Defínense ademais os seguintes roles con competencias en materia de seguridade da información:

a) Coordinador de seguridade da información: dentro do seu ámbito de actuación, é o encargado de coordinar os asuntos relativos á seguridade da información, de promover a formación e concienciación en materia de seguridade da información, de determinar as decisións que se han tomar para protexer adecuadamente a información e os servizos e de supervisar a súa implantación en todos os aspectos non relacionados coas TIC.

b) Delegado de protección de datos: desempeñará as súas funcións focalizándose nos riscos asociados ás operacións de tratamento de datos persoais, tendo en conta a natureza, o alcance, o contexto e fins do tratamento. Ten como funcións principais as que se derivan das obrigacións do cumprimento do RXPD.

5.6. Aprobación de roles e responsabilidades e resolución de conflitos.

As condicións que deben cumprir as persoas coas responsabilidades anteriores serán aprobadas segundo establece o artigo 5.j do Decreto 73/2014, do 12 de xuño, polo que se crean e se regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia.

Mentres non se establezan os mecanismos que se han seguir para a resolución de conflitos en cada un dos ámbitos de actuación a que afecte esta política, seguirase o principio de xerarquía que rexe nas administracións públicas, e será o superior xerárquico que corresponda o encargado de resolver os conflitos que poidan xurdir, sen prexuízo da independencia do delegado de protección de datos no desempeño das súas funcións, que deberá ser respectada segundo o establecido no RXPD.

6. Desenvolvemento da política de seguridade.

O corpo normativo sobre seguridade da información é de obrigado cumprimento e desenvolverase en niveis, segundo o ámbito de aplicación e o nivel de detalle técnico, de maneira que cada norma se fundamente nas normas de nivel superior. Os devanditos niveis de desenvolvemento son os seguintes:

a) Primeiro: política de seguridade da información. Está constituído polo presente documento e é de obrigado cumprimento.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

b) Segundo: políticas, plans de acción e actuacións estratéxicas en materia de seguridade da información. Está constituído polo conxunto de documentos que tratan da aplicación da presente política. Os documentos relativos a este segundo nivel normativo proporaos a Subcomisión Operativa de Seguridade á Comisión de Seguridade e Goberno Electrónico, que será quen os aprobe.

c) Terceiro: outra normativa de seguridade da información. Está constituído polo conxunto de normas que desenvolven a política de seguridade e que serven para indicar como se debe actuar. As disposicións de ámbito transversal que non estean baixo a competencia doutros órganos serán aprobadas pola Subcomisión de Seguridade.

d) Cuarto: procedementos de seguridade. Conxunto de documentos que describen explicitamente e paso a paso como se ha realizar unha certa actividade. A responsabilidade de aprobación destes procedementos dependerá do seu ámbito de aplicación, que poderá ser nun ámbito específico ou nun sistema de información determinado.

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

7. Xestión da seguridade.

7.1. Xestión de riscos.

1) A xestión de riscos é unha parte esencial do proceso de seguridade e debe realizarse de maneira continua sobre os sistemas de información, co obxectivo de manter os ámbitos controlados e de minimizar os riscos ata niveis aceptables.

2) A xestión de riscos será preceptiva para os sistemas de información incluídos dentro do marco establecido polo Real decreto 3/2010, do 8 de xaneiro, polo que se regula o ENS no ámbito da Administración electrónica, e será opcional para o resto dos supostos.

3) Os responsables da información e do servizo son os responsables dos riscos sobre a información e os servizos, respectivamente, e serán os que aseguran o seu seguimento

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

e control, sen prexuízo da posibilidade de delegar estas tarefas. Para iso, poderán contar no proceso coa participación e co asesoramento do responsable da seguridade TIC e do responsable do sistema.

4) Para a realización da análise de riscos teranse en conta as recomendacións publicadas para o ámbito da Administración pública e, en especial, as guías elaboradas polo Centro Criptolóxico Nacional.

5) A avaliación dos riscos repetirase regularmente para os sistemas de información, dentro do alcance indicado no punto dous deste número, consonte as recomendacións formuladas polo Centro Criptolóxico Nacional.

6) A avaliación de impacto relativa á protección de datos de carácter persoal será de necesaria realización nos termos establecidos no RXPD.

7.2. Deberes do persoal.

1) Todo o persoal ten o deber de cumprir a política de seguridade da información e a normativa de seguridade derivada. O seu incumprimento poderá ser sancionado de conformidade coa normativa disciplinaria correspondente.

2) Todo persoal que empregue sistemas de tecnoloxías da información e as comunicacións recibirá formación para o manexo seguro dos devanditos sistemas.

8. Concienciación e formación.

1) Correspóndelle á Subcomisión de Seguridade promover a formación e a concienciación en materia de seguridade da información no ámbito da Administración xeral do sector público autonómico de Galicia.

2) Desenvolveranse actividades específicas orientadas á formación e á concienciación de todo o persoal en materia de seguridade da información, así como á difusión da política de seguridade da información e do seu desenvolvemento normativo, e estarán dirixidas en particular ao persoal de nova incorporación.

3) Para estes efectos, os plans de formación incluirán actividades específicas sobre seguridade da información.

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

9. Glosario.

Activo	Funcionalidade ou compoñente que teña valor para a organización. Inclúe: información, datos, servizos, aplicacións, equipamentos, comunicacións, recursos administrativos, recursos físicos e recursos humanos.
Ameaza	Causa potencial dun incidente que pode causar danos a un sistema de información ou a unha organización. (UNE 71504:2008). As ameazas sempre están presentes, pero pódense intentar evitar ou paliar os efectos da súa materialización.
Análise de riscos	Proceso para a análise das ameazas, vulnerabilidades, riscos e impactos a que está exposto un sistema de información, tendo en conta as medidas de seguridade xa presentes. Serve como punto de partida para identificar as melloras nas medidas de seguridade, tanto no que se refire á efectividade coma aos custos.
Autenticidade	Propiedade ou característica consistente en que unha entidade é quen di ser ou ben que garante a fonte de que proceden os datos. (ENS).
Avaliación de impacto relativa á protección de datos (PIA)	Proceso que permite ás organizacións identificar os riscos que un sistema, produto ou servizo pode implicar para os dereitos e liberdades das persoas e, tras realizar esa análise, afrontar e xestionar eses perigos antes de que se materialicen. (RXPD).
Confidencialidade	Propiedade ou característica consistente en que a información nin se pon á disposición nin se revela a individuos, entidades ou procesos non autorizados. (ENS).
Corpo normativo	Conxunto de normas que desenvolven de forma máis concreta a maneira de alcanzar os obxectivos dunha política.
Dato de carácter persoal	Calquera información concernente a persoas físicas identificadas ou identificables. (LOPD).
Dispoñibilidade	Propiedade ou característica dos activos consistente en que as entidades ou os procesos autorizados teñen acceso a estes cando o requiren. (ENS).
Incidente ou incidencia de seguridade	Suceso inesperado ou non desexado con consecuencias negativas para a seguridade do sistema de información. (ENS).
Integridade	Propiedade ou característica consistente en que o activo de información non foi alterado de maneira non autorizada. (ENS).
LOPD	Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
Medidas de seguridade	Conxunto de disposicións encamiñadas a protexerse dos riscos posibles sobre o sistema de información, co fin de asegurar os seus obxectivos de seguridade. Pode tratarse de medidas de prevención, disuasión, protección, detección e reacción, ou ben de recuperación. (ENS).
Política de seguridade	Documento de alto nivel que especifica os obxectivos en materia de seguridade dunha organización e reflicte o compromiso da dirección para alcanzalos.
Proceso	Conxunto organizado de actividades que se levan a cabo para producir un produto ou servizo; ten un principio e unha fin delimitados, implica recursos e dá lugar a un resultado. (ENS).
RLOPD	Regulamento de desenvolvemento da LOPD, aprobado polo Real decreto 1720/2007, do 21 de decembro.
Risco	Estimación do grao de exposición a que unha ameaza se materialice sobre un ou máis activos, con danos ou perdas para a organización. (ENS).

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7

Risco residual	Risco remanente no sistema tras a implantación dunhas determinadas salvagardas no plan de tratamento de riscos.
Seguridade da información	Protección da información e dos sistemas de información fronte ao acceso, uso, divulgación, alteración, modificación ou destrución non autorizados.
Sistema de información	Conxunto organizado de recursos para que a información se poida recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, poñer á disposición, presentar ou transmitir. (ENS).
Soporte	Medio físico de calquera tipo (papel, DVD, discos portátiles, etc.) utilizado para almacenar información.
Rastrexabilidade	Propiedade ou característica consistente en que as actuacións dunha entidade poden ser imputadas exclusivamente á devandita entidade. (ENS).
Vulnerabilidade	Unha debilidade que pode ser aproveitada por unha ameaza. (ENS).
Xestión de continuidade	Actividades que leva a cabo unha organización para asegurar que todos os procesos de negocio críticos estarán dispoñibles para os seus usuarios, clientes, provedores e outras entidades que deban utilizalos.
Xestión de incidentes	Procesos orientados a recuperar o nivel habitual de funcionamento do servizo e a minimizar en todo o posible o impacto negativo na organización, de forma que se manteñan a calidade do servizo e a dispoñibilidade.
Xestión de riscos	Actividades coordinadas para dirixir e controlar unha organización con respecto aos riscos. (ENS).

CVE-DOG: wlthihc4-nba2-s4v8-31h8-0h3glfr327f7