Rivas Cruz, José Luis e cinco deputados/as máis
Sobre o recoñecemento polo Goberno galego dos montes veciñais en man común como unha titularidade veciñal, comunitaria, distinta e en condicións de igualdade coas titularidades públicas e privadas e o seu traslado á lexislación autonómica vixente, así como sobre a demanda que respecto disto debe realizar ao Goberno central
BOPG nº 215, do 22.11.2017

Sométese a votación e resulta rexeitada por 5 votos a favor, 7 votos en contra e 0 abstencións.

- 20514 (10/PNC-001669)
Grupo Parlamentario de En Marea
Rodríguez Estévez, David e Quinteiro Araújo, Paula
Sobre as actuacións que debe levar a cabo o Goberno galego en relación coas axudas convocadas para o ano 2017 para garantir a subministración de auga ás explotacións agrarias
BOPG nº 219, do 29.11.2017

Sométese a votación e resulta rexeitada por 5 votos a favor, 7 votos en contra e 0 abstencións.

Santiago de Compostela, 15 de decembro de 2017
Eva Solla Fernández
Vicepresidenta 2ª

3. Administración do Parlamento de Galicia

3.1. Organización e normas de funcionamento da Administración do Parlamento de Galicia

3.1.1. Normas e acordos

Acordo da Mesa do Parlamento de Galicia, do 13 de decembro de 2017, polo que se regula a política de seguridade da información do Parlamento de Galicia

Exposición de motivos

As leis 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas, e 40/2015, do 1 de outubro, do réxime xurídico do sector público, establecen que a tramitación electrónica dos procedementos debe constituír a acción habitual de todas as administracións, tanto na súa relación cos cidadáns como na xestión interna e nos intercambios de información entre diferentes organismos. Tamén salientan o documento, arquivo e ficheiro electrónico, que requiren afondar na transformación dixital das administracións públicas, co consecuente aumento da eficiencia e calidade dos servizos prestados aos cidadáns.

Entre os seus obxectivos tamén está a creación de condicións de confianza no uso dos medios electrónicos. Establece as medidas necesarias para a preservación da integridade dos dereitos fundamentais, especialmente aqueles relacionados coa privacidade e protección de datos persoais, garantindo a seguridade dos sistemas electrónicos, datos, comunicacións e servizos.

Estes obxectivos foron desenvolvidos polo Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Sistema Nacional de Seguridade (en diante, ENS) no ámbito da administración electrónica. Así mesmo, a información procesada nos sistemas electrónicos a que se refire o ENS estará protexida tendo en conta os criterios establecidos na Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal. O ENS, pola súa banda, establece o marco regulador da política de seguridade da información, que está incorporado nun documento, accesible e comprensible para todos os membros, que define o que significa a seguridade da información nunha determinada organización e que regula o xeito en que unha organización xestiona e protexe información e servizos críticos. A política de seguridade debe xerarse de acordo cos requisitos da ENS, que establece que todos os órganos superiores das administracións públicas deben ter oficialmente unha política de seguridade da información aprobada polo órgano superior competente.

Tendo en conta o anterior, a Mesa do Parlamento de Galicia, na súa sesión do 13 de decembro de 2018 e ao abeiro do establecido no artigo 17 do Regulamento de organización e funcionamento da Administración do Parlamento de Galicia (BOPG núm. 657, do 10 de xuño de 2016), dispón:

CAPÍTULO I. Obxecto e principios do sistema de seguridade

Artigo 1. *Obxecto*

1. A finalidade destas normas é regular a política de seguridade da información (en diante, política de seguridade) do Parlamento de Galicia (en diante, PG) e o establecemento dun marco organizativo e tecnolóxico para iso.

2. A seguridade entenderase composta por un proceso integral que consiste en todos os elementos técnicos, humanos, materiais e organizativos relacionados cos sistemas de información, excluíndo calquera tipo de accións específicas ou tratamento a curto prazo. Debe ser coñecido e cumprido por todos os usuarios dos sistemas de información do PG, con independencia da posición, cargo e responsabilidade dentro deste.

3. O Parlamento de Galicia depende dos sistemas TIC (tecnoloxías de información e comunicacións) para alcanzar os seus obxectivos. Estes sistemas deben ser administrados con dilixencia, tomando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados que poidan afectar a dispoñibilidade, integridade, confidencialidade, autenticidade e rastrexabilidade da información tratada ou os servizos prestados.

4. O obxectivo da seguridade da información é garantir a calidade da información e a prestación continuada dos servizos, actuando preventivamente, supervisando a actividade diaria e reaccionando con presteza aos incidentes.

5. Os sistemas TIC deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na confidencialidade, integridade, dispoñibilidade, uso previsto e valor da información e os servizos. Para defenderse destas ameazas, requírese unha estratexia que se adapte aos cambios nas condicións do contorno para garantir a prestación continua dos servizos. Isto implica que os departamentos deben aplicar as medidas mínimas de seguridade exixidas polo Esquema Nacional de Seguridade, así como realizar un seguimento continuo dos niveis de prestación de servizos, se-

guir e analizar as vulnerabilidades reportadas, e preparar unha resposta efectiva aos incidentes para garantir a continuidade dos servizos prestados.

6. Os diferentes departamentos deben asegurarse de que a seguridade TIC é unha parte integral de cada etapa do ciclo de vida do sistema, desde a súa concepción ata a súa retirada de servizo, pasando polas decisións de desenvolvemento ou adquisición e as actividades de explotación. Os requisitos de seguridade e as necesidades de financiamento deben ser identificados e incluídos na planificación, na solicitude de ofertas, e en pregos de licitación para proxectos de TIC.

7. Os departamentos deben estar preparados para previr, detectar, reaccionar e recuperarse de incidentes, de acordo ao artigo 7 do ENS.

Artigo 2. *Principios do sistema de seguridade*

A) Prevención

1. Os departamentos deben evitar, ou polo menos previr na medida do posible, que a información ou os servizos se vexan prexudicados por incidentes de seguridade. Para iso os departamentos deben aplicar as medidas mínimas de seguridade determinadas polo ENS, así como calquera control adicional identificado a través dunha avaliación de ameazas e riscos. Estes controis, e os roles e responsabilidades de seguridade de todo o persoal, deben estar claramente definidos e documentados.

2. Para garantir o cumprimento da política, os departamentos deben:

a) Autorizar os sistemas antes de entrar en operación.

b) Avaliar regularmente a seguridade, incluíndo avaliacións dos cambios de configuración realizados de forma rutineira.

c) Solicitar a revisión periódica por parte de terceiros co fin de obter unha avaliación independente.

B) Detección

1. Dado que os servizos se poden degradar rapidamente debido a incidentes, que van desde unha simple desaceleración ata a súa detención, os servizos deben monitorizar a operación de maneira continua para detectar anomalías nos niveis de prestación dos servizos e actuar en consecuencia segundo o establecido no artigo 9 do ENS.

2. A monitorización é especialmente relevante cando se establecen liñas de defensa de acordo co artigo 8 do ENS. Estableceranse mecanismos de detección, análise e reporte que cheguen aos responsables regularmente e cando se produce unha desviación significativa dos parámetros que se tivesen preestablecido como normais.

C) Resposta

Os departamentos deben:

a) Establecer mecanismos para responder eficazmente aos incidentes de seguridade.

b) Designar un punto de contacto para as comunicacións con respecto a incidentes detectados noutros departamentos ou noutros organismos.

c) Establecer protocolos para o intercambio de información relacionada co incidente. Isto inclúe comunicacións, en ambos os sentidos, cos equipos de resposta a emerxencias (CERT).

D) Recuperación

Para garantir a dispoñibilidade dos servizos, dispoñeranse os medios e técnicas necesarios que garantan a recuperación dos servizos máis críticos.

Artigo 3. *Alcance*

Esta política aplícase a todos os sistemas TIC do Parlamento de Galicia e a todos os usuarios dos sistemas da información da institución, sen excepcións.

Artigo 4. *Misión*

O Parlamento de Galicia, como soporte dos principios de seguridade da información establecidos segundo o Esquema Nacional de Seguridade, ofrece os seguintes obxectivos de partida:

a) Fomentar a relación electrónica da cidadanía co Parlamento de Galicia.

b) Reducir os tempos de espera de atención á cidadanía.

c) Acurtar os tempos de espera na resolución de trámites solicitados pola cidadanía.

d) Mellorar o uso interno dos sistemas de información do Parlamento de Galicia.

e) Desenvolver un sistema de xestión de información documental que facilite un rápido acceso do persoal do Parlamento de Galicia á información solicitada pola cidadanía, garantindo a seguridade da información en canto á súa integridade, confidencialidade, autenticidade, rastrexabilidade e dispoñibilidade.

f) Cumprir cos requisitos exixidos pola normativa nacional de protección de datos de carácter persoal e de impulso das administracións públicas.

g) Manter, operar e evolucionar un sistema de xestión da seguridade.

Artigo 5. *Marco normativo*

Esta política enmárcase na seguinte lexislación aplicable, sen prexuízo da aplicación da lexislación autonómica que corresponda e da normativa propia do Parlamento de Galicia:

-Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da administración electrónica.

-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.

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

-Resolución do 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.

-Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.

-Real decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, de protección de datos de carácter persoal.

-Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e do comercio electrónico.

-Lei 9/2014, do 9 de maio, xeral de telecomunicacións.

-Real decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos.

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

-Lei 25/2007, do 18 de outubro, de conservación de datos relativos ás comunicacións electrónicas e ás redes públicas de comunicacións.

-Real decreto lexislativo 1/1996, do 12 de abril, polo que se aproba o Texto refundido da Lei de propiedade intelectual.

-Real decreto lexislativo 5/2015, do 30 de outubro, polo que se aproba o texto refundido da Lei do estatuto básico do empregado público.

-Lei 59/2003, do 19 de decembro, de sinatura electrónica.

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

-Lei 56/2007, do 28 de decembro, de medidas de impulso da sociedade da información.

-Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno.

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

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

-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).

-Lei 9/2017, do 8 de novembro, de contratos do sector público, pola que se transpoñen ao ordenamento xurídico español as Directivas do Parlamento Europeo e do Consello 2014/23/UE e 2014/24/UE, do 26 de febreiro de 2014.

CAPÍTULO II. Organización da seguridade

Artigo 6. *Comité Coordinador de Seguridade TIC*

1. O Comité Coordinador de Seguridade TIC é o máximo responsable de seguridade da información e servizos. Este comité terá a seguinte composición:

a) O responsable da información de administración electrónica.

b) O responsable do Servizo de Tecnoloxías da Información.

c) Os responsables dos servizos electrónicos.

d) O responsable do Servizo de Persoal e Réxime Interior .

e) O responsable de seguridade da información.

f) A delegada de protección de datos.

2. O secretario do Comité de Seguridade TIC será o responsable do Servizo de Tecnoloxías da Información, que se encargará de convocar as reunións do Comité e levantar acta delas.

3. O Comité de Seguridade TIC informará á Mesa do Parlamento de Galicia e, indicadas no RD 3/2010, terá as seguintes funcións:

a) Coordinar e aprobar as accións en materia de seguridade da información, o que inclúe, cando menos, unha revisión anual da política de seguridade.

b) Impulsar a cultura en seguridade da información.

c) Garantir a divulgación da política e normativa de seguridade da organización.

d) Participar na categorización dos sistemas e na análise de riscos.

e) Revisar a documentación relacionada coa seguridade da información.

f) Resolver discrepancias e problemas que poidan xurdir na xestión da seguridade.

g) Desenvolver o procedemento de designación de roles.

Artigo 7. *Roles. Funcións e responsabilidades*

A) A persoa responsable da información

As súas funcións son as seguintes:

a) Establecer os requisitos da información en materia de seguridade.

b) Identificar, avaliar e aprobar a información dos cidadáns, ou doutras administracións públicas, que sexa tratada polo PG.

c) Ter en conta o estado de seguridade da información tratada.

d) Comunicar ao goberno da organización a necesidade de suspender un servizo por aquelas violacións de seguridade que afectasen a información tratada.

e) Traballar en colaboración coa persoa responsable de seguridade e a persoa responsable de sistemas no mantemento dos sistemas catalogados segundo o anexo I do Esquema Nacional de Seguridade.

B) As persoas responsables dos servizos

As súas funcións son as seguintes:

a) Establecer os requisitos dos servizos TI en materia de seguridade.

b) Identificar, avaliar e aprobar os servizos tecnolóxicos prestados polo PG aos cidadáns, ou a outras administracións públicas.

c) Ter en conta o estado de seguridade dos servizos prestados.

d) Comunicar ao goberno da organización a necesidade de suspender un servizo por aquelas violacións de seguridade que afectasen o propio servizo.

e) Traballar en colaboración co responsable de seguridade e os responsables de sistemas no mantemento dos sistemas catalogados segundo o anexo I do Esquema Nacional de Seguridade.

C) A persoa responsable de seguridade da información

As súas funcións son as seguintes:

a) Aconsellar aos responsables correspondentes na identificación da información e os servizos, así como na avaliación dos niveis de seguridade necesarios para a información e o servizo.

b) Realizar a categorización do sistema no PG.

c) Elaborar a política de seguridade.

d) Realizar análises de risco dos sistemas de información segundo determinan as normas de seguridade anexas ao Esquema Nacional de Seguridade.

e) Elaborar o documento de aplicabilidade do Esquema Nacional de Seguridade.

f) Establecer as medidas de seguridade de acordo co nivel de seguridade resultante.

g) Elaborar os documentos cos procedementos operativos de xestión da seguridade, así como a normativa de uso dos medios que será aprobada pola dirección.

h) Revisar a posta en marcha dos procedementos de xestión de seguridade, así como a súa avaliación no transcurso do ciclo de vida dos sistemas de información.

i) Elaborar os plans de mellora da seguridade.

D) A persoa responsable do Sistema TI

As súas funcións son as seguintes:

a) A implantación de medidas de seguridade de carácter técnico que tería estipulado como necesarias o responsable de seguridade.

b) A implantación dos plans de continuidade do servizo, asesorado polo responsable de seguridade.

c) A xestión, configuración e actualización, segundo corresponda, do hardware e software no que se basean mecanismos e servizos de seguridade do sistema de información.

d) A xestión das autorizacións concedidas aos usuarios do sistema, en particular os privilexios concedidos, incluído o control de que a actividade desenvolvida no sistema cumpre co que está autorizado.

e) A aplicación dos procedementos operativos de seguridade.

f) A aprobación dos cambios na configuración actual do sistema de información.

g) Asegurarse de que se cumpran os controis de seguridade establecidos estritamente.

h) Asegurarse de que se aplican os procedementos aprobados para xestionar o sistema de información.

i) Supervisar as instalacións de hardware e software, as súas modificacións e melloras para asegurar que a seguridade non sexa comprometida e en todo momento cumpren coas autorizacións relevantes.

j) A monitorización do estado de seguridade do sistema, sempre polas ferramentas e mecanismos de xestión de eventos de seguridade e auditorías técnicas que se implementaron.

E) A persoa delegada de protección de datos

As súas funcións son as seguintes:

a) Informar e asesorar o responsable ou o encargado do tratamento e os empregados que se ocupen do tratamento das obrigas que lles incumben en virtude do RXPD e doutras disposicións de protección de datos da Unión ou dos Estados membros.

b) Supervisar o cumprimento do disposto no Regulamento, doutras disposicións de protección de datos da Unión ou dos Estados membros e das políticas do responsable ou do encargado do tratamento en materia de protección de datos persoais.

c) Ofrecer o asesoramento que se lle solicite acerca da avaliación de impacto relativa á protección de datos e supervisar a súa aplicación.

d) Cooperar coa autoridade de control.

e) Actuar como punto de contacto coa autoridade de control para cuestións relativas ao tratamento.

Artigo 8. *Resolución de conflitos*

1. No caso de conflito entre as diferentes partes, este será resolto polo seu superior xerárquico. En ausencia do anterior, prevalecerá a decisión do responsable de seguridade.

2. A persoa delegada de protección de datos informará directamente á Mesa do Parlamento de Galicia.

Artigo 9. *Procedementos de designación*

As designación para os distintos roles detállanse a continuación:

a) A persoa titular de Oficialia Maior terá o rol de responsable da información do PG.

b) A persoa titular do Servizo de Persoal e Réxime Interior terá o rol de responsable dos servizos do PG.

c) A persoa titular do Servizo de Tecnoloxías da Información terá o rol responsable de seguridade da información.

d) A persoa responsable dos sistemas TI será nomeado polo letrado oficial maior do PG a proposta do Comité Coordinador de Seguridade TIC.

e) Os nomeamentos serán revisados cada dous anos ou cando un dos postos quede vacante.

Artigo 10. *Obrigas do persoal*

1. Todos os usuarios dos sistemas da información do Parlamento de Galicia teñen a obriga de coñecer e cumprir esta política de seguridade da información e a normativa de seguridade. É respon-

sabilidade do Comité de Seguridade TIC dispoñer os medios necesarios para que a información chegue aos afectados.

2. Establecerase un programa de concienciación continua para atender a todos os usuarios dos sistemas da información do Parlamento de Galicia, en particular aos de nova incorporación.

3. As persoas con responsabilidade no uso, operación ou administración de sistemas TIC recibirán formación para o manexo seguro dos sistemas na medida en que a necesiten para realizar o seu traballo. A formación será obrigatoria antes de asumir unha responsabilidade, tanto se é a súa primeira asignación ou se se trata dun cambio de posto de traballo ou de responsabilidades nel.

4. O manifesto incumprimento da política de seguridade da Información ou da normativa e os procedementos derivados delas poden levar ao inicio de medidas disciplinarias adecuadas e, se é o caso, a outras medidas legais de aplicación.

Artigo 11. *Política de seguridade da información*

Será misión do Comité Coordinador de Seguridade TIC a revisión anual desta política de seguridade da información e a proposta de revisión ou mantemento da mesma. A política será aprobada pola Mesa do Parlamento de Galicia e difundida para que a coñezan todas as partes afectadas.

Artigo 12. *Normativa e procedementos de seguridade da información*

Será misión do Comité Coordinador de Seguridade TIC a revisión e mantemento das normas técnicas de seguridade e procedementos técnicos de seguridade da información. As normas e procedementos técnicos de seguridade serán aprobados polo propio Comité Coordinador de Seguridade TIC e difundidos para que a coñezan todas as partes afectadas.

Artigo 13. *Cualificación da documentación*

1. Para facilitar o nivel de privacidade dos documentos do propio sistema de xestión da seguridade (política, normativa,...) establécense 4 niveis de privacidade:

a) Pública: información que se pode difundir libremente dentro e fóra do organismo e cuxa divulgación non afecta a institución en termos de perda de imaxe e/ou económica.

b) Interna: información que, sen ser confidencial nin restrinxida, debe manterse no ámbito interno do organismo e non debe estar dispoñible externamente, excepto a terceiras partes involucradas, con previo compromiso de confidencialidade e coñecemento do propietario dela.

c) Restrinxida: información sensible, interna a áreas ou proxectos aos que debe ter acceso controlado un grupo reducido de persoas e non toda a organización.

d) Confidencial: información de alta sensibilidade que debe ser protexida pola súa relevancia sobre decisións estratéxicas, impacto financeiro, oportunidades de negocio, potencial de fraude ou requisitos legais.

2. Calquera información non clasificada tratarase por defecto como interna, polo que a súa divulgación deberá estar autorizada polo seu propietario.

3. Para a súa etiquetaxe, designarase un código na cabeceira do documento para identificar o nivel de exposición: Ref.PUB = pública; Ref.INT = interna; Ref.RES = reservado; e Ref.CONF = confidencial.

CAPÍTULO III. Protección de datos, formación e xestión

Artigo 14. *Datos de carácter persoal*

1. O Parlamento de Galicia trata datos de carácter persoal. O documento de seguridade do PG, ao que terán acceso só as persoas autorizadas, recolle os ficheiros afectados e os responsables correspondentes.

2. Todos os sistemas de información do PG se axustarán aos niveis de seguridade requiridos pola normativa para a natureza e finalidade dos datos de carácter persoal recollidos no mencionado documento de seguridade, conforme o título VIII das medidas de seguridade no tratamento de datos de carácter persoal do Real decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.

Artigo 15. *Xestión de riscos*

1. Todos os sistemas suxeitos a esta política deberán realizar unha análise de riscos, avaliando as ameazas e os riscos aos que están expostos. Esta análise repetirase:

a) Regularmente, polo menos unha vez ao ano.

b) Cando cambie a información manexada.

c) Cando cambien os servizos prestados.

d) Cando ocorra un incidente grave de seguridade.

e) Cando se reporten vulnerabilidades graves.

2. A persoa responsable de seguridade establecerá unha valoración de referencia para os diferentes tipos de información manexados e os diferentes servizos prestados, que elaborará conxuntamente co responsable de sistema TI e os administradores da seguridade (sistemas e comunicación), e comunicará ao Comité Coordinador da Seguridade TIC.

3. O Comité Coordinador de Seguridade TIC dinamizará a dispoñibilidade de recursos para atender ás necesidades de seguridade dos diferentes sistemas, promovendo investimentos de carácter horizontal.

Artigo 16. *Desenvolvemento da política de seguridade da información*

1. Esta política desenvolverase por medio de normativa de seguridade que afronte aspectos específicos. A normativa de seguridade estará á disposición de todos os usuarios dos sistemas da infor-

mación da institución que necesiten coñecela, en particular para aqueles que utilicen, operen ou administren os sistemas de información e comunicacións.

2. A normativa de seguridade estará dispoñible na intranet do Parlamento de Galicia (http://intranet) e impresa nas dependencias do Servizo de Tecnoloxías da Información.

Artigo 17. *Terceiras partes*

1. Cando o Parlamento de Galicia preste servizos a outros organismos ou manexe información doutros organismos, faraos partícipes desta política de seguridade da información e establecerá canles para reporte e coordinación dos respectivos comités de seguridade TIC e procedementos de actuación para a reacción ante incidentes de seguridade.

2. Cando o Parlamento de Galicia utilice servizos de terceiros ou ceda información a terceiros, faraos partícipes desta política de seguridade e da normativa de seguridade que incumba os devanditos servizos ou información. A dita terceira parte quedará suxeita ás obrigas establecidas na citada normativa, e poderá desenvolver os seus propios procedementos operativos para satisfacela. Estableceranse procedementos específicos de reporte e resolución de incidencias.

3. Garantirase que o persoal de terceiros está adecuadamente concienciado en materia de seguridade, polo menos ao mesmo nivel que o establecido nesta política.

4. Cando algún aspecto da política non poida ser satisfeito por unha terceira parte segundo se require nos parágrafos anteriores, requirirase un informe da persoa responsable de seguridade que precise os riscos en que se incorre e a forma de tratalos. Requirirase a aprobación deste informe polos responsables da información e os servizos afectados antes de seguir adiante.

5. Para os efectos de intercambiar experiencias e obter asesoramento para a mellora das prácticas e controis de seguridade, o PG poderá manter contactos periódicos con organismos ou entidades especializadas en temas de seguridade como poden ser o INCIBE, CCN e outros.

Disposición derrogatoria única. *Derrogación normativa*

Esta disposición administrativa deixa sen efecto calquera acordo ou norma en materia de política de seguridade adoptados pola Mesa do Parlamento de Galicia, nomeadamente o Acordo da Mesa do Parlamento de Galicia do 20 de maio de 2014 polo que se implanta un sistema de xestión de seguridade da información do Parlamento de Galicia.

Disposición derradeira única. *Entrada en vigor*

Esta disposición administrativa entrará en vigor o día seguinte ao da súa publicación no Boletín Oficial do Parlamento de Galicia.

Santiago de Compostela, 14 de decembro de 2017

Diego Calvo Pouso
Vicepresidente 1º