

DON JOSÉ LUIS ALMAU SUPERVÍA, SECRETARIO XERAL DA EXCMA. DEPUTACIÓN PROVINCIAL DA CORUÑA

CERTIFICA: Que o Pleno da Deputación Provincial da Coruña na sesión plenaria ordinaria celebrada o vinte e seis de maio de dous mil dezasete aprobou o seguinte:


"19.-APROBACIÓN DA POLÍTICA DE SEGURIDADE DA INFORMACIÓN DA DEPUTACIÓN PROVINCIAL DA CORUÑA.

Aprobar a política de seguridade da información da Deputación Provincial da Coruña que é do seguinte teor literal:

"1.Introdución

Este documento constitúe a Política de Seguridade da Información da Deputación Provincial da Coruña, en diante "A Deputación", en cumprimento do artigo 11 (Requisitos mínimos de seguridade do Real decreto 3/2010 do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica) e da medida de seguridade org.1 contemplada no anexo II do devandito Real decreto.

Neste sentido, o mencionado artigo 11 establece que "Todos os órganos superiores das Administracións públicas deberán dispor formalmente da súa política de seguridade, que será aprobada polo titular do órgano superior correspondente."



A estrutura deste documento segue as pautas establecidas pola guía CCN-STIC-805 (publicada polo Centro Criptolóxico Nacional, ente adscrito ao Centro Nacional de Intelixencia) para a redacción da Política de Seguridade no ámbito do Esquema Nacional de Seguridade.

A Política de Seguridade da Información recolle a postura da Deputación en canto á seguridade da información e establece os criterios xerais que deben rexer a actividade do organismo en canto á seguridade.

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.

Os sistemas de información deben estar protexidos contra ameazas de rápida evolución con potencial para incidir na dispoñibilidade, integridade, confidencialidade, autenticidade, trazabilidade, uso previsto e valor da información e os servizos. Para defenderse destas ameazas, requírese unha estratexia que se adapte aos cambios nas condicións da contorna para garantir a prestación continua dos servizos.

Isto implica que se deben aplicar as medidas de seguridade esixidas polo Esquema Nacional de Seguridade e a Lei orgánica de protección de datos (en diante ENS e


LOPD), así como realizar un seguimento continuo dos niveis de prestación de servizos, seguir e analizar as vulnerabilidades reportadas, e preparar unha resposta efectiva aos incidentes para garantir a continuidade dos servizos prestados.

2. Misión da Deputación da Coruña

A Deputación da Coruña é unha institución de goberno local que promove o desenvolvemento e o benestar da cidadanía nos municipios que compoñen a provincia da Coruña. Actúa prestando servizos directamente aos cidadáns e sobre todo en cooperación cos concellos. A Deputación, ten como misión a asistencia técnica, económica e material aos concellos para que poidan prestar servizos locais de calidade de forma homoxénea en toda a provincia, coordinando servizos e organizando servizos públicos de carácter supramunicipal.

3. Marco Normativo

A normativa a que está sometida a Deputación da Coruña, máis relacionada coa súa actividade, recóllese a continuación (por orde cronolóxica ascendente):

- 
- Lei 7/85 reguladora das bases de réxime local.
 - Real decreto 2568/1986, do 28 de novembro, polo que se aproba o Regulamento de organización, funcionamento e réxime xurídico das entidades locais.
 - Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
 - Lei 33/2003, do 3 de novembro, do patrimonio das administracións públicas.
 - Real decreto legislativo 2/2004, do 5 de marzo, polo que se aproba o texto refundido da Lei reguladora das facendas locais.
 - 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.
 - Real decreto 3/2010, do 8 de xaneiro, polo que se regula o esquema nacional de seguridade no ámbito da administración electrónica.
 - Real decreto 4/2010, do 8 de xaneiro, polo que se regula o esquema nacional de interoperabilidade no ámbito da administración electrónica.
 - Real decreto legislativo 3/2011, do 14 de novembro, polo que se aproba o texto refundido da Lei de contratos do sector público.
 - Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno.
 - Lei 27/2013 de racionalización e sustentabilidade da administración local.
 - Orde HAP/2425/2013, do 23 de decembro, pola que se publican os límites dos distintos tipos de contratos a efectos da contratación do sector público a partir do 1 de xaneiro de 2014.
 - Real decreto-lei 8/2014, do 4 de xullo, de aprobación de medidas urxentes para o crecemento, a competitividade e a eficiencia.
 - Lei 18/2014, do 15 de outubro, de aprobación de medidas urxentes para o crecemento, a competitividade e a eficiencia.

- Lei 39/2015, do 1 de outubro, de procedemento administrativo común das administracións públicas.
- Lei 40/2015, do 1 de outubro de réxime xurídico do sector público.

4. Política Xeral de Seguridade

O obxecto da presente política é establecer a postura da Deputación respecto da seguridade que afecta os procesos relacionados co desempeño das súas funcións e, moi particularmente, cos relacionados coa administración electrónica, tanto desde o punto de vista das persoas usuarias dos servizos, como desde o punto de vista interno, para a xestión da propia entidade.

A Deputación utiliza as tecnoloxías da información e as comunicacións para prestar os seus servizos, polo que é consciente de que estes sistemas deben ser administrados con dilixencia, tomando as medidas adecuadas para protexelos fronte a danos accidentais ou deliberados.

Así mesmo, tamén é consciente de que os incidentes de seguridade poden estar provocados desde lugares remotos, a través das conexións a redes de comunicacións das que se dispón e, moi concretamente, a través das conexións á internet (cíber-ataques).

O fin da política é contrarrestar as ameazas mencionadas anteriormente cos medios suficientes, dentro das posibilidades orzamentarias. Para este fin, establecerase unha estrutura de seguridade, xunto cos mecanismos apropiados para a súa xestión, e un conxunto de instrumentos de apoio de forma que se garanta:

- o cumprimento dos obxectivos da súa misión e de prestación de servizos
- o cumprimento da lexislación e normativa aplicables

Para iso,

- preveranse e despregarán medidas para evitar incidentes de seguridade que puidesen afectar o cumprimento de obxectivos ou poñer en risco a información.
- deseñaranse medidas de resposta ante incidentes de seguridade, física ou lóxica, de forma que se minimice o seu impacto, no caso de que ocorresen.

Como norma xeral, terase un enfoque de orientación ao risco á hora de deseñar as medidas de seguridade necesarias, poñendo máis foco e esforzo na mitigación do que supoña un maior risco.

As distintas unidades baixo cuxa responsabilidade están os servizos prestados deberán contemplar a seguridade desde o mesmo momento en que se concibe un novo sistema ou servizo, aplicando para estes e para os xa existentes, as medidas de seguridade prescritas polo esquema nacional de seguridade para garantir a dispoñibilidade, confidencialidade, integridade, autenticidade e trazabilidade dos servizos e da información.

Os requisitos de seguridade dos sistemas, as necesidades e requisitos de formación dos usuarios, e as necesidades de financiamento deben ser identificados e incluídos na planificación dos sistemas e nos pregos de prescricións utilizados para a realización de proxectos que involucren ás tecnoloxías da información e comunicacións (TIC).

Débense articular mecanismos de prevención, reacción e recuperación con obxecto de minimizar o impacto dos incidentes de seguridade.

En canto á prevención, débese evitar que os servizos e a información resulten afectados por un incidente de seguridade. Para iso, a Deputación implementará as medidas de seguridade establecidas no anexo II do ENS, así como medidas adicionais que puidesen ser identificadas o proceso de análise de riscos.

En canto á reacción, estableceranse mecanismos de detección, comunicación e xestión de incidentes de seguridade, de forma que calquera incidente poida ser tratado no menor prazo posible. Sempre que sexa posible, detectaranse de forma automática os incidentes de seguridade, utilizando elementos de monitorización dos servizos ou de detección de anomalías e poñendo en marcha os procedementos de resposta ao incidente no menor prazo posible. Para os incidentes detectados polas persoas usuarias, xa sexan internos ou externos, estableceranse as pertinentes canles de comunicación de incidentes.

En canto á recuperación, para aqueles servizos que se consideren críticos, en base á valoración que deles realicen os seus responsables, deberanse desenvolver plans que permitan a continuidade dos devanditos servizos no caso de que, por mor dun incidente de seguridade, quedasen indispoñibles.



5. Alcance

Esta política de seguridade é de aplicación a todos os servizos prestados pola Deputación así como a todo o persoal, sen excepcións.

6. Organización da seguridade

A seguridade na Deputación está soportada sobre as estruturas e roles que se describen a continuación:

- Estrutura de especificación, que é a que se encarga de establecer os requisitos de seguridade asociados aos servizos prestados.
- Estrutura de supervisión, que é a que se encarga de verificar o cumprimento dos requisitos de seguridade e o aliñamento continuo cos obxectivos da organización.
- Estrutura de operación, que se encarga de implantar as medidas de seguridade identificadas.

6.1 Estrutura de especificación

Esta estrutura é a encargada de determinar os requisitos de seguridade que serán de aplicación aos servizos prestados pola Deputación e a garantir o cumprimento normativo asociado que lle é de aplicación, en concreto o Real decreto 3/2010 do 8 de xaneiro polo que se regula o esquema nacional de seguridade.

Forman parte desta estrutura:

- A Presidencia da Deputación.
- Os responsables dos diferentes Servizos da Deputación.
- O Comité de Seguridade.

6.2 Estrutura de supervisión

A estrutura de supervisión da seguridade encárgase de verificar a correcta implantación e operación dos requisitos de seguridade que se estableceron, de cara a manter a aliñación cos obxectivos e de cumprir coas normas e lexislación aplicable.

Na supervisión global de todas as actividades relativas á seguridade da información está o responsable de seguridade da información.

Na supervisión global das actividades relativas á seguridade física está o responsable de seguridade física.

Para a coordinación global e integral da seguridade está o Comité de Seguridade.

As funcións e responsabilidades de cada unha das figuras descríbense a continuación:

6.2.1 Responsable de Seguridade da Información

É responsable da definición, coordinación, difusión e verificación dos requisitos de seguridade da información na Deputación.

Este responsable forma parte do Comité de Seguridade e, por tanto, é o encargado de elevar ao devandito Comité os asuntos de interese relacionados coa seguridade da información.

As súas responsabilidades comprenden:

- Coordinar e controlar as medidas de seguridade da información e de protección de datos da Deputación.
- Supervisar a implantación, manter, controlar e verificar o cumprimento das normas e procedementos establecidos.
- Conseguir que se elabore o presuposto anual de seguridade de tecnoloxías da información e as comunicacións (TIC) da Deputación.

- Definir un modelo de xestión da seguridade aliñado coa estratexia da Deputación en materia de seguridade. A este modelo de xestión chamaráselle SXSI (Sistema de Xestión de Seguridade da Información), independentemente de que estea baseado nas normas internacionais que recomendan como facelo, ou se trate dun modelo diferente.
- Supervisar a implantación práctica da estratexia de seguridade da información da Deputación.
- Supervisar as situacións excepcionais (ou incidentes) de ciberseguridade producidas na Deputación.
- Promover a realización de análise de riscos de seguridade da información de forma periódica.
- Promover e coordinar a realización de programas de formación e sensibilización en materia de seguridade da información.
- Analizar os indicadores de seguridade para medir a eficacia e eficiencia das medidas implantadas.
- Analizar os incidentes de seguridade da información reflectidos nos rexistros destes e verificar que se estableceron os plans para a súa resolución.
- Manter actualizada a documentación asociada á xestión da seguridade da información: normativas, procedementos e rexistros.
- Autorizar por escrito a execución de procedementos de recuperación de datos nos casos en que se requira.
- Colaborar coas auditorías externas/internas en materia de seguridade da información, revisalas e encargar aos responsables dos sistemas a implantación das correccións que se deriven.

Desempeñará o cargo de responsable de seguridade da información o xefe de Servizo de Informática e Administración Electrónica.

6.2.2 Responsable de Seguridade Física

É responsable da definición, coordinación, difusión e verificación dos requisitos de seguridade física das instalacións onde se aloxen os sistemas de información.

Este responsable forma parte do Comité de Seguridade e, por tanto, é o encargado de elevar ao devandito Comité os asuntos de interese relacionados coa seguridade física dos locais e as infraestruturas, designados como críticos.

As súas responsabilidades comprenden:

- Identificación de necesidades de seguridade física.
- Conseguir a elaboración dun orzamento anual de investimentos e actuacións en seguridade física.
- Supervisar a instalación e o mantemento posterior dos elementos e servizos destinados á seguridade física.
- Analizar os incidentes de seguridade física que se poidan producir e establecer actuacións para dar resposta a estes.
- Manter actualizada a documentación asociada á xestión da física: normativas, procedementos e rexistros.


Desempeñará o cargo de responsable de seguridade física o xefe de Servizo de Sistemas e Soporte.

6.2.3 Comité de Seguridade

A misión do Comité de Seguridade é a coordinación xeral das actividades que teñen relación coa seguridade integral.

Un obxectivo fundamental do Comité de Seguridade é a posta en común de aspectos importantes da seguridade entre todos os responsables. Con iso evítase que actividades referentes á seguridade, que poidan afectar a varias ou todas as unidades da organización, queden sen o suficiente coñecemento por parte dos seus responsables, ou sen o suficiente apoio ou compromiso, prexudicando a eficacia.

As funcións do Comité de Seguridade son:

- 
- Informar regularmente o estado da seguridade á Presidencia.
 - Revisar regularmente a política de seguridade e propor cambios, se procede.
 - Revisar as normativas internas de seguridade que se poidan derivar da política de seguridade e propoñer para a súa aprobación.
 - Elaborar e propor os requisitos de formación para a persoa clave que manexa información, sistemas e infraestruturas físicas.
 - Propor para a súa aprobación os plans de mellora da seguridade que xurdan por mor das análises de riscos realizados.
 - Seguir o desenvolvemento dos plans de acción aprobados.
 - Coordinar as actuacións en materia de seguridade que se poidan estar a realizar en diferentes unidades da Deputación con obxecto de evitar esforzos duplicados ou desaliñados coa política de seguridade
 - Analizar incidentes de seguridade significativos. Decidir que facer por mor deles. Algúns poden comportar unha actuación con gasto, nese caso propoñase para a súa aprobación.
 - Analizar información de indicadores de seguridade que puidese haber definidos. Tomar decisións en caso de desviación respecto dos límites establecidos.
 - Propor solucións de seguridade que deban ter un orzamento aprobado.

Serán membros fixos do Comité de Seguridade:

- A Presidencia da Deputación
- O responsable de Seguridade da Información
- O responsable de Seguridade Física
- Os responsables dos diferentes Servizos da Deputación

Adicionalmente, poderán asistir ao Comité de Seguridade os responsables das materias específicas a tratar nas reunións, que poderán ser convidados en función do contido da axenda.

6.3 Estrutura de Operación

A estrutura de operación da seguridade debe asumir a administración operativa da seguridade dos sistemas de información, implantando nos devanditos sistemas as medidas necesarias para satisfacer os requisitos de seguridade establecidos pola estrutura de especificación.

Descríbense, a continuación, as funcións e responsabilidades das figuras asociadas á estrutura de operación.

6.3.1 Responsable dos Sistemas de Información

As súas funcións e responsabilidades son:

- Definir, en coordinación co responsable de seguridade da información, as especificacións funcionais de seguridade dos sistemas de información da Deputación.
- Garantir que no deseño de sistemas de información e redes de comunicacións se contemplen, desde o principio, os aspectos necesarios de seguridade da información en canto a dispoñibilidade, integridade, confidencialidade, autenticación, control de acceso, auditoría e rexistro.
- Revisar que a configuración de seguridade tras a instalación dun sistema novo é a adecuada (perfil inicial de seguridade. Bastionado).
- Revisar que a configuración de seguridade tras os cambios nun sistema segue sendo a adecuada.
- Verificar o funcionamento de mecanismos de control de acceso que eviten que un usuario acceda a datos ou recursos con dereitos distintos dos autorizados, sen que en ningún caso se poidan desactivar.
- Seguir os foros de vulnerabilidades e elaboración do calendario de aplicación de parches para os sistemas de información, en función dos que xurdan e o impacto que teñan na seguridade (os parches mesmos aplicaranos os administradores de sistemas).
- Implantar as medidas de seguridade que resulten dos plans de tratamento de riscos ou plans de accións correctivas por mor das auditorías de seguridade da información.
- Proporcionar datos para a alimentación de indicadores de seguridade da información.
- Supervisar os procedementos de copia de seguridade.
- Realizar auditorías técnicas periódicas da infraestrutura, sistemas e aplicacións.

Desempeñará o cargo de responsable dos Sistemas de Información o xefe de Servizo de Sistemas e Soporte.

7. Funcións e obrigacións

Á marxe das funcións e atribucións que atinxen ao persoal que integra o esquema organizativo responsable da seguridade, establécense a continuación as

obrigacións do persoal da Deputación así como daqueles terceiros que teñan acceso aos seus sistemas de información.

7.1 Funcións e obrigacións do persoal

Todo o persoal da Deputación ten a obrigaón de coñecer a política de seguridade e cumprila. O Comité de Seguridade disporá os medios para que esta política chegue aos afectados.

7.2 Funcións e obrigacións de terceiras partes

As terceiras partes (entidades externas á Deputación) que estean relacionadas coa xestión, mantemento ou explotación dos servizos prestados pola Deputación serán feitos partícipes desta política. As terceiras partes quedarán obrigadas ao cumprimento desta política e ás normativas que se poidan derivar dela.

As terceiras partes poderán desenvolver os seus propios procedementos operativos para satisfacer a política.

Deberanse establecer procedementos específicos de comunicación de incidencias para que os terceiros afectados poidan reportalas.

O persoal das terceiras partes deberá recibir sesións de concienciación, tal como se esixe para o persoal propio.

Cando algún aspecto desta política non poida ser satisfeito por unha terceira parte, o responsable de seguridade deberá realizar un informe do risco en que se incorre. Ese risco deberá ser aceptado polo Comité de Seguridade.

8. Formación e concienciación

Con carácter periódico, determinado polo Comité de Seguridade, a proposta do responsable de seguridade, realizarase unha acción de formación e concienciación en materia de seguridade.

O obxectivo da acción formativa e de concienciación é dobre:

- manter informado o persoal máis directamente relacionado co manexo de información e os sistemas que a tratan sobre os procedementos existentes de seguridade, riscos, medidas de protección, plans de protección, etc.
- concienciar o persoal en xeral da importancia da seguridade e dos procedementos básicos de manexo e intercambio de información.

O primeiro obxectivo asóciase a formación e o segundo a concienciación.

Realizarase unha sesión inicial de concienciación en materia de política de seguridade da información, á que deberá asistir todo o persoal da Deputación.

As persoas con responsabilidade no uso, a xestión, mantemento ou explotación dos servizos soportados nas 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.

9. Xestión de riscos

Os servizos e infraestruturas baixo o alcance da presente política deberán estar sometidos a unha análise de riscos para orientar as medidas de protección para minimizar estes.

Como metodoloxía base para a realización das análises de riscos utilizarase Magerit, sendo esta metodoloxía a máis recomendable para o sector público nacional.

Utilizaranse, como punto de partida, o catálogo de ameazas de seguridade previsto na metodoloxía.

A análise realizarase:

- regularmente, unha vez ao ano.
- cando haxa cambios nos servizos esenciais prestados ou cambios significativos nas infraestruturas que os soportan.
- cando ocorra un incidente de seguridade grave.
- cando se identifiquen ameazas severas que non fosen tidas en conta ou vulnerabilidades graves que non estean contrarrestadas polas medidas de protección implantadas.

De acordo coa escala de riscos da metodoloxía MAGERIT (metodoloxía de análise e xestión de riscos elaborada polo Consello Superior de Administración Electrónica), o nivel de risco deberá situarse por baixo de nivel ALTO para considerarse de forma automática como aceptable (o risco residual máximo debe ser MEDIO). Valores de risco residual maiores a MEDIO deberán ser aceptados explicitamente polo Comité de Seguridade, logo da xustificación previa da conveniencia da súa aceptación.

Para os valores de risco residual que non sexan aceptables deberase elaborar o correspondente Plan de tratamento que permita levar os valores de risco a valores aceptables.

10. Datos de carácter persoal

A Deputación só recollerá datos de carácter persoal cando sexan adecuados, pertinentes e non excesivos e estes estean en relación co ámbito e as finalidades para os que se obtiveron. De igual modo, adoptará as medidas de índole técnica e organizativas necesarias para o cumprimento da normativa de protección de datos.

Estas medidas estarán recollidas no Documento de Seguridade, que está baixo a custodia do Comité de Seguridade.

No devandito documento relaciónanse os ficheiros con datos persoais e os seus responsables, así como as persoas autorizadas para o seu acceso.

11. Desenvolvemento da política de seguridade

Esta política de seguridade desenvolverase mediante a elaboración doutras políticas ou normativas de seguridade que aborden aspectos específicos. Por mor das devanditas políticas e normativas poderanse desenvolver procedementos que describan a forma de levalas a cabo.

A documentación de políticas e normativas de seguridade, así como esta política de seguridade estará ao dispor de todo o persoal da organización que necesite coñecela e, en particular, o persoal que utilice, opere ou administre os sistemas de información e comunicacións ou a información mesma albergada nos devanditos sistemas ou os servizos prestados pola Deputación.

12. Revisión e a probación

A presente política de seguridade será revisada con carácter anual."

E para que conste e sen prexuízo dos termos da aprobación da acta, segundo o disposto no artigo 206 do Regulamento de organización, funcionamento e réxime xurídico das Corporacións locais, expido a presente de orde e co visto e praxe do Sr. Presidente na Coruña a vinte e nove de maio de dous mil dezasete.

Vº e Pr.

O PRESIDENTE

