I. DISPOSICIÓNS XERAIS

MINISTERIO DA PRESIDENCIA

11881 *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.*

A Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos, estableceu o Esquema Nacional de Seguridade que, aprobado mediante o Real decreto 3/2010, do 8 de xaneiro, ten por obxecto determinar a política de seguridade na utilización de medios electrónicos no seu ámbito de aplicación e estará constituído polos principios básicos e requisitos mínimos que permitan unha protección adecuada da información. Tamén estableceu que o citado esquema se debía manter actualizado de maneira permanente e, en desenvolvemento deste precepto, o Real decreto 3/2010, do 8 de xaneiro, establece que o Esquema Nacional de Seguridade se desenvolverá e perfeccionará ao longo do tempo en paralelo ao progreso dos servizos de Administración electrónica, a evolución da tecnoloxía, os novos estándares internacionais sobre seguridade e auditoría, e a consolidación das infraestruturas que lle serven de apoio, e que se manterá actualizado de maneira permanente.

Posteriormente, a Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público, establece que as administracións públicas se relacionarán entre si e cos seus órganos, organismos públicos e entidades vinculados ou dependentes a través de medios electrónicos que aseguren a interoperabilidade e a seguridade dos sistemas e solucións adoptadas por cada unha delas, garantirán a protección dos datos de carácter persoal e facilitarán, preferentemente, a prestación conxunta de servizos aos interesados, e recolle o Esquema Nacional de Seguridade no seu artigo 156. Mentres, a Lei 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas, recolle no seu artigo 13, sobre dereitos das persoas nas súas relacións coas administracións públicas, o relativo á protección de datos de carácter persoal e, en particular, á seguridade e confidencialidade dos datos que figuren nos ficheiros, sistemas e aplicacións das administracións públicas.

En efecto, os cidadáns confían en que os servizos públicos dispoñibles polo medio electrónico se presten nunhas condicións de seguridade equivalentes ás que encontran cando se achegan persoalmente ás oficinas da Administración.

Por outra parte, as ciberameazas, que constitúen riscos que afectan singularmente a seguridade nacional, convertéronse nun potente instrumento de agresión contra as entidades públicas e os cidadáns nas súas relacións con estas, de maneira que a ciberseguridade figura entre os doce ámbitos prioritarios de actuación da Estratexia de seguridade nacional como instrumento actualizado para encarar o constante e profundo cambio mundial en que estamos mergullados e como garantía da adecuada actuación de España no ámbito internacional. En particular, este ámbito de actuación de ciberseguridade refírese á garantía da seguridade dos sistemas de información e das redes de comunicacións e infraestruturas comúns a todas as administracións públicas e a que se finalizará a implantación do Esquema Nacional de Seguridade, previsto na Lei 11/2007, do 22 de xuño. Profundando na cuestión, a Estratexia de ciberseguridade nacional «que utilizan as administracións públicas posúe o adecuado nivel de ciberseguridade e resiliencia» e na súa liña de acción 2, titulada «Seguridade dos sistemas de información e telecomunicacións que soportan as administracións públicas», inclúese a medida relativa a «asegurar a plena implantación do Esquema Nacional de Seguridade e articular os procedementos necesarios para coñecer regularmente o estado das principais variables de seguridade dos sistemas afectados».

Por todo isto e, en particular, dada a rápida evolución das tecnoloxías de aplicación e a experiencia derivada da implantación do Esquema Nacional de Seguridade, é aconsellable a actualización desta norma, cuxo alcance e contido se orientan a precisar, profundar e contribuír ao mellor cumprimento dos mandados normativos e clarifican o papel do Centro Criptolóxico Nacional e do CCN-CERT, eliminan a referencia ao Inteco, explicitan e relacionan as instrucións técnicas de seguridade e a declaración de aplicabilidade, actualizan o anexo II, referido ás medidas de seguridade, e simplifican e concretan o anexo III, referido á auditoría de seguridade, modifican o glosario de termos recollido no anexo IV, modifican a redacción da cláusula administrativa particular contida no anexo V e finalizan establecendo mediante disposición transitoria un prazo de vinte e catro meses contados a partir da entrada en vigor para a adecuación dos sistemas ao disposto na modificación.

Nese senso modifícanse o número 1 do artigo 11, o número 3 do 15, o título do 18, o seu número 1 e engádese un novo número 4, a alínea a) do 19, o número 2 do 24, o 27 mediante a introdución de dous novos números 4 e 5, o título do 29, os seus números 1 e 2 e introdúcese un novo número 3, os artigos 35 e 36, a alínea 1.a) do 37, os anexos II a V, elimínase a disposición adicional segunda, modifícase a numeración das disposicións adicionais terceira e cuarta e engádese unha nova disposición adicional cuarta.

Todo isto coa dita finalidade e para adecuarse ao previsto no Regulamento n.º 910/2014 do Parlamento Europeo e do Consello, do 23 de xullo de 2014, relativo á identificación electrónica e aos servizos de confianza para as transaccións electrónicas no mercado interior e polo que se derroga a Directiva 1999/93/CE.

Na súa virtude, por proposta do ministro de Facenda e Administracións Públicas e da ministra da Presidencia, de acordo co Consello de Estado e logo de deliberación do Consello de Ministros na súa reunión do día 23 de outubro de 2015,

DISPOÑO:

Artigo único. *Modificación do Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración electrónica.*

O Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración electrónica, queda modificado no seguinte sentido:

Un. O número 1 do artigo 11 queda redactado como segue:

«Todos os órganos superiores das administracións públicas deberán dispor formalmente da súa política de seguridade que articule a xestión continuada da seguridade, que será aprobada polo titular do órgano superior correspondente. Esta política de seguridade establecerase de acordo cos principios básicos indicados e desenvolverase aplicando os seguintes requisitos mínimos:

a) Organización e implantación do proceso de seguridade.
b) Análise e xestión dos riscos.
c) Xestión de persoal.
d) Profesionalidade.
e) Autorización e control dos accesos.
f) Protección das instalacións.
g) Adquisición de produtos.
h) Seguridade por defecto.
i) Integridade e actualización do sistema.
j) Protección da información almacenada e en tránsito.
k) Prevención ante outros sistemas de información interconectados.
l) Rexistro de actividade.
m) Incidentes de seguridade.

n) Continuidade da actividade.
o) Mellora continua do proceso de seguridade.»

Dous. O número 3 do artigo 15 queda redactado como segue:

«3. As administracións públicas exixirán, de maneira obxectiva e non discriminatoria, que as organizacións que lles presten servizos de seguridade conten con profesionais cualificados e cuns niveis idóneos de xestión e madureza nos servizos prestados.»

Tres. Modifícase o artigo 18, cuxo título pasa a ser «Adquisición de produtos de seguridade e contratación de servizos de seguridade», e os seus números 1 e 4 quedan redactados como segue:

«1. Na adquisición de produtos de seguridade das tecnoloxías da información e das comunicacións que vaian ser empregados polas administracións públicas utilizaranse, de forma proporcionada á categoría do sistema e nivel de seguridade determinados, aqueles que teñan certificada a funcionalidade de seguridade relacionada co obxecto da súa adquisición, salvo naqueles casos en que as exixencias de proporcionalidade canto aos riscos asumidos non o xustifiquen a xuízo do responsable de seguridade.»

«4. Para a contratación de servizos de seguridade observarase o disposto nos números anteriores e no artigo 15.»

Catro. A alínea a) do artigo 19 queda redactada como segue:

«a) O sistema proporcionará a mínima funcionalidade requirida para que a organización alcance os seus obxectivos.»

Cinco. O número 2 do artigo 24 queda redactado como segue:

«2. Disporase de procedementos de xestión de incidentes de seguridade e de debilidades detectadas nos elementos do sistema de información. Estes procedementos cubrirán os mecanismos de detección, os criterios de clasificación, os procedementos de análise e resolución, así como as canles de comunicación coas partes interesadas e o rexistro das actuacións. Este rexistro empregarase para a mellora continua da seguridade do sistema.»

Seis. Engádense dous novos números 4 e 5 ao artigo 27, redactados como segue:

«4. A relación de medidas seleccionadas do anexo II formalizarase nun documento denominado “declaración de aplicabilidade”, asinado polo responsable de seguridade.

5. As medidas de seguridade referenciadas no anexo II poderán ser substituídas por outras compensatorias sempre que se xustifique documentalmente que protexen igual ou mellor o risco sobre os activos (anexo I) e que se satisfán os principios básicos e os requisitos mínimos previstos nos capítulos II e III do real decreto. Como parte integral da declaración de aplicabilidade, indicarase de forma detallada a correspondencia entre as medidas compensatorias implantadas e as medidas do anexo II que compensan, e o conxunto será obxecto da aprobación formal por parte do responsable de seguridade.»

Sete. Modifícase o artigo 29, cuxo título pasa a ser «Instrucións técnicas de seguridade e guías de seguridade», que queda redactado como segue:

«1. Para o mellor cumprimento do establecido no Esquema Nacional de Seguridade, o Centro Criptolóxico Nacional, no exercicio das súas competencias, elaborará e difundirá as correspondentes guías de seguridade das tecnoloxías da información e das comunicacións.

2. O Ministerio de Facenda e Administracións Públicas, por proposta do Comité Sectorial de Administración Electrónica previsto no artigo 40 da Lei 11/2007, do 22 de xuño, e por iniciativa do Centro Criptolóxico Nacional, aprobará as instrucións técnicas de seguridade de obrigado cumprimento e que se publicarán mediante resolución da Secretaría de Estado de Administracións Públicas. Para a redacción e o mantemento das instrucións técnicas de seguridade constituiranse os correspondentes grupos de traballo nos órganos colexiados con competencias en materia de Administración electrónica.

3. As instrucións técnicas de seguridade terán en conta as normas harmonizadas a nivel europeo que resulten de aplicación.»

Oito. O artigo 35 queda redactado como segue:

«O Comité Sectorial de Administración Electrónica recollerá a información relacionada co estado das principais variables da seguridade nos sistemas de información a que se refire o presente real decreto, de forma que permita elaborar un perfil xeral do estado da seguridade nas administracións públicas.

O Centro Criptolóxico Nacional articulará os procedementos necesarios para a recolla e consolidación da información, así como os aspectos metodolóxicos para o seu tratamento e explotación, a través dos correspondentes grupos de traballo que se constitúan para isto no Comité Sectorial de Administración Electrónica e na Comisión de Estratexia TIC para a Administración Xeral do Estado.»

Nove. No artigo 36 engádese un segundo parágrafo coa seguinte redacción:

«As administracións públicas notificarán ao Centro Criptolóxico 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 presente real decreto.»

Dez. No artigo 37, a alínea 1.a) queda redactada como segue:

«a) Soporte e coordinación para o tratamento de vulnerabilidades e a resolución de incidentes de seguridade que teñan a Administración xeral do Estado, as administracións das comunidades autónomas, as entidades que integran a Administración local e as entidades de dereito público con personalidade xurídica propia vinculadas ou dependentes de calquera das administracións indicadas.

O CCN-CERT, a través do seu servizo de apoio técnico e de coordinación, actuará coa máxima celeridade ante calquera agresión recibida nos sistemas de información das administracións públicas.

Para o cumprimento dos fins indicados nos parágrafos anteriores poderanse pedir informes de auditoría dos sistemas afectados, rexistros de auditoría, configuracións e calquera outra información que se considere relevante, así como os soportes informáticos que se consideren necesarios para a investigación do incidente dos sistemas afectados, sen prexuízo do disposto na Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal, e na súa normativa de desenvolvemento, así como da posible confidencialidade de datos de carácter institucional ou organizativo.»

Once. Elimínase a disposición adicional segunda, «Instituto Nacional de Tecnoloxías da Comunicación (Inteco) e organismos análogos», a disposición adicional terceira pasa a ser a disposición adicional segunda e a disposición adicional cuarta a ser a disposición adicional terceira.

Doce. Engádese unha nova disposición adicional cuarta redactada como segue:

«Disposición adicional cuarta. *Desenvolvemento do Esquema Nacional de Seguridade.*

1. Sen prexuízo das propostas que poida acordar o Comité Sectorial de Administración Electrónica segundo o establecido no artigo 29, número 2, desenvolveranse as seguintes instrucións técnicas de seguridade, que serán de obrigado cumprimento para as administracións públicas:

a) Informe do estado da seguridade.
b) Notificación de incidentes de seguridade.
c) Auditoría da seguridade.
d) Conformidade co Esquema Nacional de Seguridade.
e) Adquisición de produtos de seguridade.
f) Criptoloxía de emprego no Esquema Nacional de Seguridade.
g) Interconexión no Esquema Nacional de Seguridade.
h) Requisitos de seguridade en contornos externalizados.

2. A aprobación destas instrucións realizarase de acordo co procedemento establecido no citado artigo 29, números 2 e 3.»

Trece. A táboa do número 2.4 do anexo II queda redactada como segue:

«Dimensións				Medidas de seguridade	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridade
categoría	aplica	=	=	org.2	Normativa de seguridade
categoría	aplica	=	=	org.3	Procedementos de seguridade
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análise de riscos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridade
categoría	aplica	=	=	op.pl.3	Adquisición de novos compoñentes
D	n.a.	aplica	=	op.pl.4	Dimensionamento/xestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Compoñentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funcións e tarefas
I C A T	aplica	=	=	op.acc.4	Proceso de xestión de dereitos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Acceso remoto *(remote login)*
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridade
categoría	n.a.	aplica	=	op.exp.3	Xestión da configuración
categoría	aplica	=	=	op.exp.4	Mantemento
categoría	n.a.	aplica	=	op.exp.5	Xestión de cambios
categoría	aplica	=	=	op.exp.6	Protección fronte a código daniño

«Dimensións				Medidas de seguridade	
Afectadas	B	M	A		
categoría	n.a.	aplica	=	op.exp.7	Xestión de incidentes
T	aplica	+	++	op.exp.8	Rexistro da actividade dos usuarios
categoría	n.a.	aplica	=	op.exp.9	Rexistro da xestión de incidentes
T	n.a.	n.a.	aplica	op.exp.10	Protección dos rexistros de actividade
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servizos externos
categoría	n.a.	aplica	=	op.ext.1	Contratación e acordos de nivel de servizo
categoría	n.a.	aplica	=	op.ext.2	Xestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidade do servizo
D	n.a.	aplica	=	op.cont.1	Análise de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidade
D	n.a.	n.a.	aplica	op.cont.3	Probas periódicas
				op.mon	Monitorización do sistema
categoría	n.a.	aplica	=	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección das instalacións e infraestruturas
categoría	aplica	=	=	mp.if.1	Áreas separadas e con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación das persoas
categoría	aplica	=	=	mp.if.3	Acondicionamento dos locais
D	aplica	+	=	mp.if.4	Enerxía eléctrica
D	aplica	=	=	mp.if.5	Protección fronte a incendios
D	n.a.	aplica	=	mp.if.6	Protección fronte a inundacións
categoría	aplica	=	=	mp.if.7	Rexistro de entrada e saída de equipamentos
D	n.a.	n.a.	aplica	mp.if.9	Instalacións alternativas
				mp.per	Xestión do persoal
categoría	n.a.	aplica	=	mp.per.1	Caracterización do posto de traballo
categoría	aplica	=	=	mp.per.2	Deberes e obrigacións
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Persoal alternativo
				mp.eq	Protección dos equipamentos
categoría	aplica	+	=	mp.eq.1	Posto de traballo despexado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de posto de traballo
categoría	aplica	=	+	mp.eq.3	Protección de equipamentos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección das comunicacións
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección da confidencialidade
I A	aplica	+	++	mp.com.3	Protección da autenticidade e da integridade
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección dos soportes de información
C	aplica	=	=	mp.si.1	Etiquetaxe
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	aplica	+	=	mp.si.5	Borrado e destrución

«Dimensións				Medidas de seguridade	
Afectadas	B	M	A		
				mp.sw	Protección das aplicacións informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desenvolvemento
categoría	aplica	+	++	mp.sw.2	Aceptación e posta en servizo
				mp.info	Protección da información
categoría	aplica	=	=	mp.info.1	Datos de carácter persoal
C	aplica	+	=	mp.info.2	Cualificación da información
C	n.a.	n.a.	aplica	mp.info.3	Cifraxe
I A	aplica	+	++	mp.info.4	Sinatura electrónica
T	n.a.	n.a.	aplica	mp.info.5	Selos de tempo
C	aplica	=	=	mp.info.6	Limpeza de documentos
D	aplica	=	=	mp.info.9	Copias de seguridade *(backup)*
				mp.s	Protección dos servizos
categoría	aplica	=	=	mp.s.1	Protección do correo electrónico
categoría	aplica	=	+	mp.s.2	Protección de servizos e aplicacións web
D	n.a.	aplica	+	mp.s.8	Protección fronte á denegación de servizo
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos»

Catorce. Modifícanse os números 3.4, 4.1.2, 4.1.5, 4.2.1, 4.2.5, 4.3.3, 4.3.7, 4.3.8, 4.3.9, 4.3.11, 4.4.2, 4.6.1, 4.6.2, 5.2.3, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.5, 5.6.1, 5.7.4, 5.7.5, 5.7.7 e 5.8.2 do anexo II do real decreto, nos seguintes termos:

«3.4 Proceso de autorización [org.4].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Establecerase un proceso formal de autorizacións que cubra todos os elementos do sistema de información:

a) Utilización de instalacións habituais e alternativas.
b) Entrada de equipamentos en produción, en particular, equipamentos que involucren criptografía.
c) Entrada de aplicacións en produción.
d) Establecemento de ligazóns de comunicacións con outros sistemas.
e) Utilización de medios de comunicación habituais e alternativos.
f) Utilización de soportes de información.
g) Utilización de equipamentos móbiles. Entenderase por equipamentos móbiles ordenadores portátiles, PDA ou outros de natureza análoga.
h) Utilización de servizos de terceiros, baixo contrato ou convenio.»

«4.1.2 Arquitectura de seguridade [op.pl.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	+	+

A seguridade do sistema será obxecto dun deseño integral que detalle, ao menos, os seguintes aspectos:

Categoría BÁSICA

a) Documentación das instalacións:

1. Áreas.
2. Puntos de acceso.

b) Documentación do sistema:

1. Equipamentos.
2. Redes internas e conexións co exterior.
3. Puntos de acceso ao sistema (postos de traballo e consolas de administración).

c) Esquema de liñas de defensa:

1. Puntos de interconexión con outros sistemas ou a outras redes, en especial se se trata da internet ou redes públicas en xeral.
2. Tornalumes, DMZ, etc.
3. Utilización de tecnoloxías diferentes para previr vulnerabilidades que poidan perforar simultaneamente varias liñas de defensa.

d) Sistema de identificación e autenticación de usuarios:

1. Uso de claves concertadas, contrasinais, tarxetas de identificación, biometría ou outras de natureza análoga.
2. Uso de ficheiros ou directorios para autenticar o usuario e determinar os seus dereitos de acceso.

Categoría MEDIA

e) Sistema de xestión, relativo á planificación, organización e control dos recursos relativos á seguridade da información.

Categoría ALTA

f) Sistema de xestión de seguridade da información con actualización e aprobación periódica.
g) Controis técnicos internos:

1. Validación de datos de entrada, saída e datos intermedios.»

«4.1.5 Compoñentes certificados [op.pl.5].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	non aplica	aplica

Categoría ALTA

Utilizaranse sistemas, produtos ou equipamentos cuxas funcionalidades de seguridade e o seu nivel fosen avaliados conforme normas europeas ou internacionais e cuxos certificados estean recoñecidos polo Esquema nacional de avaliación e certificación da seguridade das tecnoloxías da información.

Terán a consideración de normas europeas ou internacionais, ISO/IEC 15408 ou outras de natureza e calidade análogas.

Unha instrución técnica de seguridade detallará os criterios exixibles.»

«4.2.1 Identificación [op.acc.1].

dimensións	A T		
nivel	baixo	medio	alto
	aplica	=	=

A identificación dos usuarios do sistema realizarase de acordo co que se indica a seguir:

1. Poderanse utilizar como identificador único os sistemas de identificación previstos na normativa de aplicación.
2. Cando o usuario teña diferentes roles fronte ao sistema (por exemplo, como cidadán, como traballador interno do organismo e como administrador dos sistemas), recibirá identificadores singulares para cada un dos casos de forma que sempre queden delimitados privilexios e rexistros de actividade.
3. Cada entidade (usuario ou proceso) que accede ao sistema contará cun identificador singular de tal forma:

a) que se poida saber quen recibe e que dereitos de acceso recibe.
b) que se poida saber quen fixo algo e o que fixo.

4. As contas de usuario xestionaranse da seguinte forma:

a) Cada conta estará asociada a un identificador único.
b) As contas deben ser inhabilitadas nos seguintes casos: cando o usuario deixa a organización, cando o usuario cesa na función para a cal se requiría a conta de usuario ou cando a persoa que a autorizou dá orde en senso contrario.
c) As contas reteranse durante o período necesario para atender ás necesidades de rastrexabilidade dos rexistros de actividade asociados a elas. Este período denominarase “período de retención”.

5. Nos supostos mencionados no capítulo IV, relativo a comunicacións electrónicas, as partes intervenientes identificaranse de acordo cos mecanismos previstos na lexislación europea e nacional na materia, coa seguinte correspondencia entre os niveis da dimensión de autenticidade dos sistemas de información a que se ten acceso e os niveis de seguridade (baixo, substancial, alto) dos sistemas de identificación electrónica previstos no Regulamento n.º 910/2014 do Parlamento Europeo e do Consello, do 23 de xullo de 2014, relativo á identificación electrónica e aos servizos de confianza para as transaccións electrónicas no mercado interior e polo que se derroga a Directiva 1999/93/CE:

– Se se require un nivel BAIXO na dimensión de autenticidade (anexo I): nivel de seguridade baixo, substancial ou alto (artigo 8 do Regulamento n.º 910/2014)
– Se se require un nivel MEDIO na dimensión de autenticidade (anexo I): nivel de seguridade substancial ou alto (artigo 8 do Regulamento n.º 910/2014)
– Se se require un nivel ALTO na dimensión de autenticidade (anexo I): nivel de seguridade alto (artigo 8 do Regulamento n.º 910/2014).»

«4.2.5 Mecanismo de autenticación [op.acc.5].

dimensións	ICAT		
nivel	baixo	medio	alto
	aplica	+	++

Os mecanismos de autenticación fronte ao sistema adecuaranse ao nivel do sistema atendendo ás consideracións que seguen, e poden usarse os seguintes factores de autenticación:

– "algo que se sabe": contrasinais ou claves concertadas.
– "algo que se ten": compoñentes lóxicos (tales como certificados *software*) ou dispositivos físicos (en expresión inglesa, *tokens).*
– "algo que se é": elementos biométricos.

Os factores anteriores poderán utilizarse de maneira illada ou combinarse para xerar mecanismos de autenticación forte.

As guías CCN-STIC desenvolverán os mecanismos concretos adecuados para cada nivel.

As instancias do factor ou os factores de autenticación que se utilicen no sistema denominaranse "credenciais".

Antes de proporcionar as credenciais de autenticación aos usuarios, estes deberanse ter identificado e rexistrado de maneira fidedigna ante o sistema ou ante un fornecedor de identidade electrónica recoñecido pola Administración. Prevense varias posibilidades de rexistro dos usuarios:

– Mediante a presentación física do usuario e verificación da súa identidade acorde coa legalidade vixente, ante un funcionario habilitado para isto.
– De forma telemática, mediante DNI electrónico ou un certificado electrónico cualificado.
– De forma telemática, utilizando outros sistemas admitidos legalmente para a identificación dos cidadáns dos considerados na normativa de aplicación.

Nivel BAIXO

a) Como principio xeral, admitirase o uso de calquera mecanismo de autenticación sustentado nun só factor.
b) No caso de se utilizar como factor "algo que se sabe", aplicaranse regras básicas de calidade.
c) Atenderase á seguridade das credenciais da seguinte forma:

1. As credenciais activaranse unha vez que estean baixo o control efectivo do usuario.
2. As credenciais estarán baixo o control exclusivo do usuario.
3. O usuario recoñecerá que as recibiu e que coñece e acepta as obrigacións que implica telas, en particular, o deber de custodia dilixente, protección da súa confidencialidade e información inmediata en caso de perda.
4. As credenciais cambiaranse cunha periodicidade marcada pola política da organización, atendendo á categoría do sistema a que se accede.
5. As credenciais retiraranse e serán deshabilitadas cando a entidade (persoa, equipamento ou proceso) que autentican termina a súa relación co sistema.

Nivel MEDIO

a) Exixirase o uso de, ao menos, dous factores de autenticación.
b) No caso de utilización de "algo que se sabe" como factor de autenticación, estableceranse exixencias rigorosas de calidade e renovación.
c) As credenciais utilizadas deberán ter sido obtidas após un rexistro previo:

1. Presencial.
2. Telemático, usando certificado electrónico cualificado.
3. Telemático, mediante unha autenticación cunha credencial electrónica obtida após un rexistro previo presencial ou telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de sinatura.

Nivel ALTO

a) As credenciais suspenderanse após un período definido sen se utilizaren.
b) No caso de se utilizar “algo que se ten”, requirirase o uso de elementos criptográficos *hardware* usando algoritmos e parámetros acreditados polo Centro Criptolóxico Nacional.
c) As credenciais utilizadas deberanse obter após un rexistro previo presencial ou telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de sinatura.»

«4.3.3 Xestión da configuración [op.exp.3].

Dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Categoría MEDIA

Xestionarase de forma continua a configuración dos compoñentes do sistema de forma:

a) Que se manteña en todo momento a regra de «funcionalidade mínima» ([op.exp.2]).
b) Que se manteña en todo momento a regra de «seguridade por defecto» ([op.exp.2]).
c) Que o sistema se adapte ás novas necesidades, previamente autorizadas ([op.acc.4]).
d) Que o sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).
e) Que o sistema reaccione a incidentes (ver [op.exp.7]).»

«4.3.7 Xestión de incidentes [op.exp.7].

Dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Categoría MEDIA

Disporase dun proceso integral para facer fronte aos incidentes que poidan ter un impacto na seguridade do sistema, incluíndo:

a) Procedemento de reporte de eventos de seguridade e debilidades, detallando os criterios de clasificación e a escalada da notificación.
b) Procedemento de toma de medidas urxentes, incluíndo a detención de servizos, o illamento do sistema afectado, a recolla de evidencias e a protección dos rexistros, segundo conveña ao caso.
c) Procedemento de asignación de recursos para investigar as causas, analizar as consecuencias e resolver o incidente.
d) Procedementos para informar as partes interesadas, internas e externas.
e) Procedementos para:

1. Previr que se repita o incidente.
2. Incluír nos procedementos de usuario a identificación e a forma de tratar o incidente.

3. Actualizar, estender, mellorar ou optimizar os procedementos de resolución de incidentes.

A xestión de incidentes que afecten datos de carácter persoal terá en conta o disposto na Lei orgánica 15/1999, do 13 de decembro, e normas de desenvolvemento, sen prexuízo de cumprir, ademais, as medidas establecidas por este real decreto.»

«4.3.8 Rexistro da actividade dos usuarios [op.exp.8].

dimensións	T		
nivel	baixo	medio	alto
	aplica	+	++

Rexistraranse as actividades dos usuarios no sistema da seguinte forma:

a) O rexistro indicará quen realiza a actividade, cando a realiza e sobre que información.
b) Incluirase a actividade dos usuarios e, especialmente, a dos operadores e administradores en canto poidan acceder á configuración e actuar no mantemento do sistema.
c) Deberán rexistrarse as actividades realizadas con éxito e as tentativas fracasadas.
d) A determinación de que actividades deben rexistrarse e con que niveis de detalle se adoptará á vista da análise de riscos realizada sobre o sistema ([op.pl.1]).

Nivel BAIXO

Activaranse os rexistros de actividade nos servidores.

Nivel MEDIO

Revisaranse informalmente os rexistros de actividade buscando patróns anormais.

Nivel ALTO

Disporase dun sistema automático de recolección de rexistros e correlación de eventos; é dicir, unha consola de seguridade centralizada.»

«4.3.9 Rexistro da xestión de incidentes [op.exp.9].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Categoría MEDIA

Rexistraranse todas as actuacións relacionadas coa xestión de incidentes da seguinte forma:

a) Rexistrarase o reporte inicial, as actuacións de emerxencia e as modificacións do sistema derivadas do incidente.
b) Rexistrarase aquela evidencia que poida, posteriormente, sustentar unha demanda xudicial ou facerlle fronte, cando o incidente poida levar a actuacións disciplinarias contra o persoal interno, contra fornecedores externos ou á

persecución de delitos. Na determinación da composición e detalle destas evidencias recorrerase a asesoramento legal especializado.

c) Como consecuencia da análise dos incidentes, revisarase a determinación dos eventos auditables.»

«4.3.11 Protección de claves criptográficas [op.exp.11].

dimensións	Todas		
categoría	básica	media	alta
	aplica	+	=

As claves criptográficas protexeranse durante todo o seu ciclo de vida: (1) xeración, (2) transporte ao punto de explotación, (3) custodia durante a explotación, (4) arquivamento posterior á súa retirada de explotación activa e (5) destrución final.

Categoría BÁSICA

a) Os medios de xeración estarán illados dos medios de explotación.

b) As claves retiradas de operación que deban ser arquivadas, serano en medios illados dos de explotación.

Categoría MEDIA

a) Usaranse programas avaliados ou dispositivos criptográficos certificados conforme o establecido en [op.pl.5].

b) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.»

«4.4.2 Xestión diaria [op.ext.2].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Categoría MEDIA

Para a xestión diaria do sistema estableceranse os seguintes puntos:

a) Un sistema rutineiro para medir o cumprimento das obrigacións de servizo e o procedemento para neutralizar calquera desviación fóra da marxe de tolerancia acordada ([op.ext.1]).

b) O mecanismo e os procedementos de coordinación para levar a cabo as tarefas de mantemento dos sistemas afectados polo acordo.

c) O mecanismo e os procedementos de coordinación en caso de incidentes e desastres (ver [op.exp.7]).»

«4.6.1 Detección de intrusión [op.mon.1].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Categoría MEDIA

Disporase de ferramentas de detección ou de prevención de intrusión.»

«4.6.2 Sistema de métricas [op.mon.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:

Recompilaranse os datos necesarios atendendo á categoría do sistema para coñecer o grao de implantación das medidas de seguridade que apliquen das detalladas no anexo II e, se for o caso, para prover o informe anual requirido polo artigo 35.

Categoría MEDIA:

Ademais, recompilaranse datos para valorar o sistema de xestión de incidentes que permitan coñecer

– O número de incidentes de seguridade tratados.
– O tempo empregado para fechar o 50% dos incidentes.
– O tempo empregado para fechar o 90% dos incidentes.

Categoría ALTA

Recompilaranse datos para coñecer a eficiencia do sistema de seguridade TIC:

– Recursos consumidos: horas e orzamento.»

«5.2.3 Concienciación [mp.per.3].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Realizaranse as accións necesarias para concienciar regularmente o persoal acerca do seu papel e responsabilidade para que a seguridade do sistema alcance os niveis exixidos.
En particular, lembrarase regularmente:

a) A normativa de seguridade relativa ao bo uso dos sistemas.
b) A identificación de incidentes, actividades ou comportamentos sospeitosos que deban ser reportados para o seu tratamento por persoal especializado.
c) O procedemento de reporte de incidentes de seguridade, sexan reais ou falsas alarmas.»

«5.3.3 Protección de portátiles [mp.eq.3].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Os equipamentos que sexan susceptibles de saír das instalacións da organización e non se poidan beneficiar da protección física correspondente, cun risco manifesto de perda ou roubo, serán protexidos adecuadamente.

Sen prexuízo das medidas xerais que os afecten, adoptaranse as seguintes:

a) Levarase un inventario de equipamentos portátiles xunto cunha identificación da persoa responsable e un control regular de que está positivamente baixo o seu control.

b) Establecerase unha canle de comunicación para informar o servizo de xestión de incidentes de perdas ou subtraccións.

c) Cando un equipamento portátil se conecte remotamente a través de redes que non están baixo o estrito control da organización, o ámbito de operación do servidor limitará a información e os servizos accesibles aos mínimos imprescindibles, que requirirá autorización previa dos responsables da información e dos servizos afectados. Este punto é de aplicación a conexións a través da internet e doutras redes que non sexan de confianza.

d) Evitarase, na medida do posible, que o equipamento conteña claves de acceso remoto á organización. Considerararanse claves de acceso remoto aquelas que sexan capaces de habilitar un acceso a outros equipamentos da organización, ou outras de natureza análoga.

Categoría ALTA

a) Dotarase o dispositivo de detectores de violación que permitan saber se o equipamento foi manipulado e activen os procedementos previstos de xestión do incidente.

b) A información de nivel alto almacenada no disco protexerase mediante cifraxe.»

«5.4.2 Protección da confidencialidade [mp.com.2].

dimensións	C		
nivel	baixo	medio	alto
	non aplica	aplica	+

Nivel MEDIO

a) Empregaranse redes privadas virtuais cando a comunicación discorra por redes fóra do propio dominio de seguridade.

b) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.

Nivel ALTO

a) Empregaranse, preferentemente, dispositivos *hardware* no establecemento e utilización da rede privada virtual.

b) Empregaranse produtos certificados conforme o establecido en [op.pl.5].»

«5.4.3 Protección da autenticidade e da integridade [mp.com.3].

dimensións	I A		
nivel	baixo	medio	alto
	aplica	+	++

Nivel BAIXO

a) Asegurarase a autenticidade do outro extremo dunha canle de comunicación antes de intercambiar información (ver [op.acc.5]).
b) Previranse ataques activos, garantindo que, ao menos, serán detectados e que se activarán os procedementos previstos de tratamento do incidente Consideraranse ataques activos:

1. A alteración da información en tránsito.
2. A inxección de información espuria.
3. O secuestro da sesión por unha terceira parte.

c) Aceptarase calquera mecanismo de autenticación dos previstos na normativa de aplicación.

Nivel MEDIO

a) Empregaranse redes privadas virtuais cando a comunicación discorra por redes fóra do propio dominio de seguridade.
b) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.
c) Aceptarase calquera mecanismo de autenticación dos previstos na normativa de aplicación. En caso de uso de claves concertadas, aplicaranse exixencias medias canto á súa calidade fronte a ataques de adiviñación, dicionario ou forza bruta.

Nivel ALTO

a) Valorarase positivamente o emprego de dispositivos *hardware* no establecemento e utilización da rede privada virtual.
b) Empregaranse produtos certificados conforme o establecido en [op.pl.5].
c) Aceptarase calquera mecanismo de autenticación dos previstos na normativa de aplicación. En caso de uso de claves concertadas, aplicaranse exixencias altas canto á súa calidade fronte a ataques de adiviñación, dicionario ou forza bruta.»

«5.5.2 Criptografía [mp.si.2].

dimensións	I C		
nivel	baixo	medio	alto
	non aplica	aplica	+

Esta medida aplícase, en particular, a todos os dispositivos removibles. Entenderanse por dispositivos removibles os CD, os DVD, os discos USB ou outros de natureza análoga.

Nivel MEDIO

Aplicaranse mecanismos criptográficos que garantan a confidencialidade e a integridade da información contida.

Nivel ALTO

a) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.
b) Empregaranse produtos certificados conforme o establecido en [op.pl.5].»

«5.5.5 Borrado e destrución [mp.si.5].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	+	=

A medida de borrado e destrución de soportes de información aplicarase a todo tipo de equipamentos susceptibles de almacenar información, incluíndo medios electrónicos e non electrónicos.

Nivel BAIXO

a) Os soportes que vaian ser reutilizados para outra información ou liberados a outra organización serán obxecto dun borrado seguro do seu contido.

Nivel MEDIO

b) Destruiranse de forma segura os soportes nos seguintes casos:

1. Cando a natureza do soporte non permita un borrado seguro.
2. Cando así o requira o procedemento asociado ao tipo de información contida.

c) Empregaranse produtos certificados conforme o establecido en ([op. pl.5]).»

«5.6.1 Desenvolvemento de aplicacións [mp.sw.1].

dimensións	Todas		
categoría	baixa	media	alta
	non aplica	aplica	=

Categoría MEDIA

a) O desenvolvemento de aplicacións realizarase sobre un sistema diferente e separado do de produción e non deben existir ferramentas ou datos de desenvolvemento no contorno de produción.

b) Aplicarase unha metodoloxía de desenvolvemento recoñecida que:

1.º Tome en consideración os aspectos de seguridade ao longo de todo o ciclo de vida.
2.º Trate especificamente os datos usados en probas.
3.º Permita a inspección do código fonte.
4.º Inclúa normas de programación segura.

c) Os seguintes elementos serán parte integral do deseño do sistema:

1.º Os mecanismos de identificación e autenticación.
2.º Os mecanismos de protección da información tratada.
3.º A xeración e o tratamento de pistas de auditoría.

d) As probas anteriores á implantación ou modificación dos sistemas de información non se realizarán con datos reais, salvo que se asegure o nivel de seguridade correspondente.»

«5.7.4 Sinatura electrónica [mp.info.4].

dimensións	I A		
nivel	baixo	medio	alto
	aplica	+	++

Empregarase a sinatura electrónica como un instrumento capaz de permitir a comprobación da autenticidade da procedencia e a integridade da información e de ofrecer as bases para evitar o repudio.

A integridade e a autenticidade dos documentos garantiranse por medio de sinaturas electrónicas cos condicionantes que se describen a seguir, proporcionados aos niveis de seguridade requiridos polo sistema.

No caso de que se utilicen outros mecanismos de sinatura electrónica suxeitos a dereito, o sistema debe incorporar medidas compensatorias suficientes que ofrezan garantías equivalentes ou superiores no relativo á prevención do repudio, usando o procedemento previsto no punto 5 do artigo 27.

Nivel BAIXO

Empregarase calquera tipo de sinatura electrónica dos previstos na lexislación vixente.

Nivel MEDIO

a) Cando se empreguen sistemas de sinatura electrónica avanzada baseados en certificados, estes serán cualificados.

b) Empregaranse algoritmos e parámetros acreditados polo Centro Criptolóxico Nacional.

c) Garantirase a verificación e a validación da sinatura electrónica durante o tempo requirido pola actividade administrativa que aquela soporte, sen prexuízo de que se poida ampliar este período de acordo co que estableza a política de sinatura electrónica e de certificados que sexa de aplicación. Para tal fin:

d) Xuntarase á sinatura, ou referenciarase, toda a información pertinente para a súa verificación e validación:

1. Certificados.
2. Datos de verificación e validación.

e) O organismo que recolla documentos asinados polo administrado verificará e validará a sinatura recibida no momento da recepción, anexando ou referenciando sen ambigüidade a información descrita nas epígrafes 1 e 2 da alínea d).

f) A sinatura electrónica de documentos por parte da Administración anexará ou referenciará sen ambigüidade a información descrita nas epígrafes 1 e 2.

Nivel ALTO

1. Usarase sinatura electrónica cualificada, incorporando certificados cualificados e dispositivos cualificados de creación de sinatura.
2. Empregaranse produtos certificados conforme o establecido en [op.pl.5].»

«5.7.5 Selos de tempo [mp.info.5].

dimensións	T		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Nivel ALTO

Os selos de tempo previrán a posibilidade do repudio posterior:

1. Os selos de tempo aplicaranse a aquela información que sexa susceptible de ser utilizada como evidencia electrónica no futuro.
2. Os datos pertinentes para a verificación posterior da data serán tratados coa mesma seguridade que a información datada para efectos de dispoñibilidade, integridade e confidencialidade.
3. Renovaranse regularmente os selos de tempo ata que a información protexida xa non sexa requirida polo proceso administrativo a que dá soporte.
4. Utilizaranse produtos certificados (segundo [op.pl.5]) ou servizos externos admitidos (véxase [op.exp.10]).
5. Empregaranse «selos cualificados de tempo electrónicos» acordes coa normativa europea na materia.»

«5.7.7 Copias de seguridade (*backup*) [mp.info.9].

dimensións	D		
nivel	baixo	medio	alto
	aplica	=	=

Realizaranse copias de seguridade que permitan recuperar datos perdidos, accidental ou intencionadamente, cunha antigüidade determinada.

Estas copias posuirán o mesmo nivel de seguridade que os datos orixinais no que se refire a integridade, confidencialidade, autenticidade e rastrexabilidade. En particular, considerarase a conveniencia ou necesidade, segundo proceda, de que as copias de seguridade estean cifradas para garantir a confidencialidade.

As copias de seguridade deberán abranguer:

g) Información de traballo da organización.
h) Aplicacións en explotación, incluíndo os sistemas operativos.
i) Datos de configuración, servizos, aplicacións, equipamentos ou outros de natureza análoga.
j) Claves utilizadas para preservar a confidencialidade da información.»

«5.8.2 Protección de servizos e aplicacións web [mp.s.2].

dimensións	Todas		
nivel	básica	media	alta
	aplica	=	+

Os subsistemas dedicados á publicación de información deberán ser protexidos fronte ás ameazas que lles son propias.

a) Cando a información teña algún tipo de control de acceso, garantirase a imposibilidade de acceder á información obviando a autenticación, en particular tomando medidas nos seguintes aspectos:

1.º Evitarase que o servidor ofreza acceso aos documentos por vías alternativas ao protocolo determinado.
2.º Previranse ataques de manipulación de URL.
3.º Previranse ataques de manipulación de fragmentos de información que se almacenan no disco duro do visitante dunha páxina web a través do seu navegador, por petición do servidor da páxina, coñecido en terminoloxía inglesa como *cookies*.

4.º Previranse ataques de inxección de código.

b) Previranse tentativas de escalada de privilexios.
c) Previranse ataques de *cross site scripting*.
d) Previranse ataques de manipulación de programas ou dispositivos que realizan unha acción en representación doutros, coñecidos en terminoloxía inglesa como *proxies,* e sistemas especiais de almacenamento de alta velocidade, coñecidos en terminoloxía inglesa como *caches*.

Nivel BAIXO

Empregaranse "certificados de autenticación de sitio web" acordes coa normativa europea na materia.

Nivel ALTO

Empregaranse "certificados cualificados de autenticación do sitio web" acordes coa normativa europea na materia.»

Quince. O anexo III, titulado «Auditoría da seguridade», queda redactado como segue:

«1. Obxecto da auditoría.

1.1 A seguridade dos sistemas de información dunha organización será auditada nos seguintes termos:

a) A política de seguridade define os roles e funcións dos responsables da información, os servizos, os activos e a seguridade do sistema de información.
b) Existen procedementos para resolución de conflitos entre os ditos responsables.
c) Designáronse persoas para os ditos roles á luz do principio de "separación de funcións".
d) Realizouse unha análise de riscos, con revisión e aprobación anual.
e) Cúmprense as recomendacións de protección descritas no anexo II, sobre medidas de seguridade, en función das condicións de aplicación en cada caso.
f) Existe un sistema de xestión da seguridade da información, documentado e cun proceso regular de aprobación pola dirección.

1.2 A auditoría basearase na existencia de evidencias que permitan sustentar obxectivamente o cumprimento dos puntos mencionados:

a) Documentación dos procedementos.
b) Rexistro de incidentes.
c) Exame do persoal afectado: coñecemento e praxe das medidas que o afectan.
d) Produtos certificados. Considerarase evidencia suficiente o emprego de produtos que satisfagan o establecido no artigo 18 "Adquisición de produtos e contratación de servizos de seguridade".

2. Niveis de auditoría.

Os niveis de auditoría que se realizarán aos sistemas de información serán os seguintes:

2.1 Auditoría de sistemas de categoría BÁSICA.

a) Os sistemas de información de categoría BÁSICA ou inferior non necesitarán realizar unha auditoría. Bastará unha autoavaliación realizada polo mesmo persoal que administra o sistema de información, ou en quen este delegue.

O resultado da autoavaliación debe estar documentado e indicar se cada medida de seguridade está implantada e suxeita a revisión regular e as evidencias que sustentan a valoración anterior.

b) Os informes de autoavaliación serán analizados polo responsable de seguridade competente, que elevará as conclusións ao responsable do sistema para que adopte as medidas correctoras adecuadas.

2.2 Auditoría de sistemas de categoría MEDIA ou ALTA.

a) O informe de auditoría ditaminará sobre o grao de cumprimento do presente real decreto, identificará as súas deficiencias e suxerirá as posibles medidas correctoras ou complementarias que sexan necesarias, así como as recomendacións que se consideren oportunas. Deberá, igualmente, incluír os criterios metodolóxicos de auditoría utilizados, o alcance e o obxectivo da auditoría, e os datos, feitos e observacións en que se baseen as conclusións formuladas.

b) Os informes de auditoría serán analizados polo responsable de seguridade competente, que presentará as súas conclusións ao responsable do sistema para que adopte as medidas correctoras adecuadas.

3. Interpretación.

A interpretación do presente anexo realizarase segundo o senso propio das súas palabras, en relación co contexto, antecedentes históricos e lexislativos, entre os cales figura o disposto na instrución técnica CCN-STIC correspondente, atendendo ao espírito e finalidade daquelas.»

Dezaseis. Modifícase o anexo IV, titulado «Glosario». A definición de xestión de incidentes queda como segue:

«Xestión de incidentes. Plan de acción para atender os incidentes que se dean. Ademais de resolvelos debe incorporar medidas de desempeño que permitan coñecer a calidade do sistema de protección e detectar tendencias antes de que se convertan en grandes problemas.»

Dezasete. O anexo V, relativo ao modelo de cláusula administrativa particular, queda redactado como segue:

«Cláusula administrativa particular.–En cumprimento do disposto no artigo 115.4 do Real decreto lexislativo 3/2011, do 14 de novembro, polo que se aproba o texto refundido da Lei de contratos do sector público, e no artigo 18 do Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración electrónica, o licitador incluirá referencia precisa, documentada e acreditativa de que os produtos de seguridade, servizos, equipamentos, sistemas, aplicacións ou os seus compoñentes cumpren co indicado na medida op.pl.5 sobre compoñentes certificados, recollida no número 4.1.5 do anexo II do citado Real decreto 3/2010, do 8 de xaneiro.

Cando estes sexan empregados para o tratamento de datos de carácter persoal, o licitador incluirá tamén o establecido na disposición adicional única 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.»

Disposición transitoria única. *Adecuación de sistemas.*

As entidades incluídas dentro do ámbito de aplicación do presente real decreto disporán dun prazo de vinte e catro meses contados a partir da data da entrada en vigor do presente real decreto para a adecuación dos seus sistemas ao disposto nel.

Disposición derradeira única. *Entrada en vigor.*

Este real decreto entrará en vigor o día seguinte ao da súa publicación no «Boletín Oficial del Estado».

Dado en Oviedo o 23 de outubro de 2015.

FELIPE R.

A vicepresidenta do Goberno e ministra da Presidencia,
SORAYA SÁENZ DE SANTAMARÍA ANTÓN