I. DISPOSICIÓNS XERAIS

MINISTERIO DA PRESIDENCIA

1330 *Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración electrónica.*

I

A necesaria xeneralización da sociedade da información é subsidiaria, en gran medida, da confianza que xere nos cidadáns a relación a través de medios electrónicos.

No ámbito das administracións públicas, a consagración do dereito a comunicarse con elas a través de medios electrónicos comporta unha obriga correlativa destas, que ten como premisas a promoción das condicións para que a liberdade e a igualdade sexan reais e efectivas, e a remoción dos obstáculos que impidan ou dificulten a súa plenitude, o que demanda incorporar as peculiaridades que exixen unha aplicación segura destas tecnoloxías.

A isto deu resposta o artigo 42.2 da Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos, mediante a creación do Esquema Nacional de Seguridade, cuxo obxecto é o establecemento dos principios e requisitos dunha política de seguridade na utilización de medios electrónicos que permita a adecuada protección da información.

A finalidade do Esquema Nacional de Seguridade é a creación das condicións necesarias de confianza no uso dos medios electrónicos, a través de medidas para garantir a seguridade dos sistemas, os datos, as comunicacións e os servizos electrónicos, que permita aos cidadáns e ás administracións públicas o exercicio de dereitos e o cumprimento de deberes a través destes medios.

O Esquema Nacional de Seguridade persegue fundamentar a confianza en que os sistemas de información prestarán os seus servizos e custodiarán a información de acordo coas súas especificacións funcionais, sen interrupcións ou modificacións fóra de control, e sen que a información poida chegar ao coñecemento de persoas non autorizadas. Desenvolverase e perfeccionarase en paralelo á evolución dos servizos e a medida que se vaian consolidando os requisitos destes e das infraestruturas que o apoian.

Actualmente os sistemas de información das administracións públicas están fortemente imbricados entre si e con sistemas de información do sector privado: empresas e administrados. Desta maneira, a seguridade ten un novo reto que vai máis alá do aseguramento individual de cada sistema. Por iso, cada sistema debe ter claro o seu perímetro e os responsables de cada dominio de seguridade débense coordinar efectivamente para evitar lagoas e fracturas que poidan danar a información ou os servizos prestados.

Neste contexto enténdese por seguridade das redes e da información a capacidade das redes ou dos sistemas de información de resistiren, cun determinado nivel de confianza, os accidentes ou accións ilícitas ou malintencionadas que comprometan a dispoñibilidade, autenticidade, integridade e confidencialidade dos datos almacenados ou transmitidos e dos servizos que estas redes e sistemas ofrecen ou fan accesibles.

II

O Esquema Nacional de Seguridade ten presentes as recomendacións da Unión Europea (Decisión 2001/844/CE CECA, Euratom da Comisión, do 29 de novembro de 2001, pola que se modifica o seu regulamento interno e Decisión 2001/264/CE do Consello, do 19 de marzo de 2001, pola que se adoptan as normas de seguridade do Consello), a situación tecnolóxica das diferentes administracións públicas, así como os servizos

electrónicos existentes nelas, a utilización de estándares abertos e, de forma complementaria, estándares de uso xeneralizado polos cidadáns.

A súa articulación realizouse atendendo á normativa nacional sobre Administración electrónica, protección de datos de carácter persoal, sinatura electrónica e documento nacional de identidade electrónico, Centro Criptolóxico Nacional, sociedade da información, reutilización da información no sector público e órganos colexiados responsables da Administración electrónica; así como a regulación de diferentes instrumentos e servizos da Administración, as directrices e guías da OCDE e disposicións nacionais e internacionais sobre normalización.

A Lei 11/2007, do 22 de xuño, posibilita e inspira esta norma e axuda ao seu desenvolvemento nos aspectos da seguridade dos sistemas de tecnoloxías da información nas administracións públicas, contribuíndo ao desenvolvemento dun instrumento efectivo que permite garantir os dereitos dos cidadáns na Administración electrónica.

A Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal, e as súas normas de desenvolvemento determinan as medidas para a protección dos datos de carácter persoal. Ademais, proporcionan criterios para establecer a proporcionalidade entre as medidas de seguridade e a información que se deben protexer.

A Lei 30/1992, do 26 de novembro, de réxime xurídico das administracións públicas e do procedemento administrativo común, referente legal imprescindible de calquera regulación administrativa, determina a configuración de numerosos ámbitos de confidencialidade administrativos, diferentes á información clasificada e aos datos de carácter persoal, que necesitan ser materialmente protexidos. Así mesmo, determina o substrato legal das comunicacións administrativas e os seus requisitos xurídicos de validez e eficacia, sobre os cales soportar os requirimentos tecnolóxicos e de seguridade necesarios para proxectar os seus efectos nas comunicacións realizadas por vía electrónica.

A Lei 37/2007, do 16 de novembro, sobre reutilización da información do sector público determina a regulación básica do réxime xurídico aplicable á reutilización de documentos elaborados no sector público, que configura un ámbito excepcionado da súa aplicación, no cal se encontra a información a que se refire o Esquema Nacional de Seguridade.

Xunto ás disposicións indicadas, inspiraron o contido desta norma documentos da Administración en materia de seguridade electrónica, tales como os criterios de seguridade, normalización e conservación, as guías CCN-STIC de seguridade dos sistemas de información e comunicacións, a metodoloxía e ferramentas de análise e xestión de riscos ou o Esquema Nacional de Interoperabilidade, tamén desenvolvido ao abeiro do disposto na Lei 11/2007, do 22 de xuño.

III

Este real decreto limítase a establecer os principios básicos e requisitos mínimos que, de acordo co interese xeral, natureza e complexidade da materia regulada, permiten unha protección adecuada da información e os servizos, o que exixe incluír o alcance e procedemento para xestionar a seguridade electrónica dos sistemas que tratan información das administracións públicas no ámbito da Lei 11/2007, do 22 de xuño. Con isto lógrase un común denominador normativo, cuxa regulación non esgota todas as posibilidades de normación, e permite ser completada, mediante a regulación dos obxectivos, materialmente non básicos, que poderán ser decididos por políticas lexislativas territoriais.

Para dar cumprimento ao anterior determínanse as dimensións de seguridade e os seus niveis, a categoría dos sistemas, as medidas de seguridade adecuadas e a auditoría periódica da seguridade; implántase a elaboración dun informe para coñecer regularmente o estado de seguridade dos sistemas de información a que se refire este real decreto, establécese o papel da capacidade de resposta ante incidentes de seguridade da información do Centro Criptolóxico Nacional, inclúese un glosario de termos e faise unha referencia expresa á formación.

A norma estrutúrase en dez capítulos, catro disposicións adicionais, unha disposición transitoria, unha disposición derrogatoria e tres disposicións derradeiras. Aos catro

primeiros anexos dedicados á categoría dos sistemas, ás medidas de seguridade, á auditoría da seguridade, e ao glosario de termos úneselles un quinto que establece un modelo de cláusula administrativa particular para incluír nas prescricións administrativas dos contratos correspondentes.

Neste real decreto concíbese a seguridade como unha actividade integral, na cal non caben actuacións puntuais ou tratamentos conxunturais, debido a que a debilidade dun sistema a determina o seu punto máis fráxil e, con frecuencia, este punto é a coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. A información tratada nos sistemas electrónicos a que se refire este real decreto estará protexida tendo en conta os criterios establecidos na Lei orgánica 15/1999, do 13 de decembro.

Este real decreto apróbase en aplicación do disposto na disposición derradeira oitava da Lei 11/2007, do 22 de xuño e, de acordo co disposto no artigo 42, número 3 e na disposición derradeira primeira desa norma, elaborouse coa participación de todas as administracións públicas ás cales lles é de aplicación, conta co informe favorable da Comisión Permanente do Consello Superior de Administración Electrónica, a Conferencia Sectorial de Administración Pública e a Comisión Nacional de Administración Local, e foi sometido ao informe previo da Axencia Española de Protección de Datos. Así mesmo, someteuse á audiencia dos cidadáns segundo as previsións establecidas no artigo 24 da Lei 50/1997, do 27 de novembro, do Goberno.

Na súa virtude, por proposta da ministra da Presidencia, de acordo co Consello de Estado e logo de deliberación do Consello de Ministros na súa reunión do día 8 de xaneiro de 2010,

DISPOÑO:

CAPÍTULO I

Disposicións xerais

Artigo 1. *Obxecto.*

1. Este real decreto ten por obxecto regular o Esquema Nacional de Seguridade establecido no artigo 42 da Lei 11/2007, do 22 de xuño, e determinar a política de seguridade que se debe aplicar na utilización dos medios electrónicos a que se refire a citada lei.

2. O Esquema Nacional de Seguridade está constituído polos principios básicos e requisitos mínimos requiridos para unha protección adecuada da información. Será aplicado polas administracións públicas para asegurar o acceso, integridade, dispoñibilidade, autenticidade, confidencialidade, trazabilidade e conservación dos datos, informacións e servizos utilizados en medios electrónicos que xestionen no exercicio das súas competencias.

Artigo 2. *Definicións e estándares.*

Para os efectos previstos neste real decreto, as definicións, palabras, expresións e termos deben ser entendidos no sentido indicado no glosario de termos incluído no anexo IV.

Artigo 3. *Ámbito de aplicación.*

O ámbito de aplicación deste real decreto será o establecido no artigo 2 da Lei 11/2007, do 22 de xuño.

Están excluídos do ámbito de aplicación indicado no parágrafo anterior os sistemas que tratan información clasificada regulada pola Lei 9/1968, do 5 de abril, de segredos oficiais e normas de desenvolvemento.

CAPÍTULO II

Principios básicos

Artigo 4. *Principios básicos do Esquema Nacional de Seguridade.*

O obxecto último da seguridade da información é asegurar que unha organización administrativa poderá cumprir os seus obxectivos utilizando sistemas de información. Nas decisións en materia de seguridade deberanse ter en conta os seguintes principios básicos:

a) Seguridade integral.
b) Xestión de riscos.
c) Prevención, reacción e recuperación.
d) Liñas de defensa.
e) Reavaliación periódica.
f) Función diferenciada.

Artigo 5. *A seguridade como un proceso integral.*

1. A seguridade entenderase como un proceso integral constituído por todos os elementos técnicos, humanos, materiais e organizativos, relacionados co sistema. A aplicación do Esquema Nacional de Seguridade estará presidida por este principio, que exclúe calquera actuación puntual ou tratamento conxuntural.
2. Prestarase a máxima atención á concienciación das persoas que interveñen no proceso e aos seus responsables xerárquicos para que nin a ignorancia, nin a falta de organización e coordinación, nin instrucións inadecuadas, sexan fontes de risco para a seguridade.

Artigo 6. *Xestión da seguridade baseada nos riscos.*

1. A análise e xestión de riscos será parte esencial do proceso de seguridade e deberase manter permanentemente actualizada.
2. A xestión de riscos permitirá o mantemento dun contorno controlado, minimizando os riscos ata niveis aceptables. A redución destes niveis realizarase mediante o despregamento de medidas de seguridade, que establecerá un equilibrio entre a natureza dos datos e os tratamentos, os riscos a que estean expostos e as medidas de seguridade.

Artigo 7. *Prevención, reacción e recuperación.*

1. A seguridade do sistema debe ter en conta os aspectos de prevención, detección e corrección, para conseguir que as ameazas sobre el non se materialicen, non afecten gravemente a información que manexa ou os servizos que se prestan.
2. As medidas de prevención deben eliminar ou, polo menos reducir, a posibilidade de que as ameazas cheguen a se materializar con prexuízo para o sistema. Estas medidas de prevención terán presentes, entre outras, a disuasión e a redución da exposición.
3. As medidas de detección estarán acompañadas de medidas de reacción, de forma que os incidentes de seguridade se atallen a tempo.
4. As medidas de recuperación permitirán a restauración da información e dos servizos, de forma que se poida facer fronte ás situacións en que un incidente de seguridade inhabilite os medios habituais.
5. Sen mingua dos demais principios básicos e requisitos mínimos establecidos, o sistema garantirá a conservación dos datos e informacións en soporte electrónico.

De igual modo, o sistema manterá dispoñibles os servizos durante todo o ciclo vital da información dixital, a través dunha concepción e procedementos que sexan a base para a preservación do patrimonio dixital.

Artigo 8. *Liñas de defensa.*

1. O sistema debe dispor dunha estratexia de protección constituída por múltiples capas de seguridade, disposta de forma que, cando unha das capas falle, permita:

a) Gañar tempo para unha reacción adecuada fronte aos incidentes que non se puideron evitar.
b) Reducir a probabilidade de que o sistema sexa comprometido no seu conxunto.
c) Minimizar o impacto final sobre el.

2. As liñas de defensa deben estar constituídas por medidas de natureza organizativa, física e lóxica.

Artigo 9. *Reavaliación periódica.*

As medidas de seguridade reavaliaranse e actualizaranse periodicamente, para adecuar a súa eficacia á constante evolución dos riscos e sistemas de protección, chegando incluso a unha reformulación da seguridade, se for necesario.

Artigo 10. *A seguridade como función diferenciada.*

Nos sistemas de información diferenciarase o responsable da información, o responsable do servizo e o responsable da seguridade.
O responsable da información determinará os requisitos da información tratada; o responsable do servizo determinará os requisitos dos servizos prestados; e o responsable de seguridade determinará as decisións para satisfacer os requisitos de seguridade da información e dos servizos.
A responsabilidade da seguridade dos sistemas de información estará diferenciada da responsabilidade sobre a prestación dos servizos.
A política de seguridade da organización detallará as atribucións de cada responsable e os mecanismos de coordinación e resolución de conflitos.

CAPÍTULO III

Requisitos mínimos

Artigo 11. *Requisitos mínimos de seguridade.*

1. Todos os órganos superiores das administracións públicas deberán dispor formalmente da súa política de seguridade, que será aprobada polo titular do órgano superior correspondente. Esta política de seguridade establecerase con base nos 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.

2. Para os efectos indicados no número anterior, consideraranse órganos superiores os responsables directos da execución da acción do goberno, central, autonómico ou local, nun sector de actividade específico, de acordo co establecido na Lei 6/1997, do 14 de abril, de organización e funcionamento da Administración xeral do Estado, e Lei 50/1997, do 27 de novembro, do Goberno; os estatutos de autonomía correspondentes e normas de desenvolvemento, e a Lei 7/1985, do 2 de abril, reguladora das bases do réxime local, respectivamente.

Os municipios poderán dispor dunha política de seguridade común elaborada pola deputación, cabido, consello insular ou órgano unipersoal correspondente daqueloutras corporacións de carácter representativo ás cales corresponda o goberno e a administración autónoma da provincia ou, de ser o caso, á entidade comarcal correspondente a que pertenzan.

3. Todos estes requisitos mínimos se exixirán en proporción aos riscos identificados en cada sistema, e algúns poderán non requirirse en sistemas sen riscos significativos, e cumpriranse de acordo co establecido no artigo 27.

Artigo 12. *Organización e implantación do proceso de seguridade.*

A seguridade deberá comprometer a todos os membros da organización. A política de seguridade segundo se detalla no anexo II, sección 3.1, deberá identificar uns claros responsables de velar polo seu cumprimento e ser coñecida por todos os membros da organización administrativa.

Artigo 13. *Análise e xestión dos riscos.*

1. Cada organización que desenvolva e implante sistemas para o tratamento da información e as comunicacións realizará a súa propia xestión de riscos.

2. Esta xestión realizarase por medio da análise e do tratamento dos riscos a que está exposto o sistema. Sen prexuízo do disposto no anexo II, empregarase algunha metodoloxía recoñecida internacionalmente.

3. As medidas adoptadas para mitigar ou suprimir os riscos deberán estar xustificadas e, en todo caso, existirá unha proporcionalidade entre elas e os riscos.

Artigo 14. *Xestión de persoal.*

1. Todo o persoal relacionado coa información e cos sistemas deberá ser formado e informado dos seus deberes e obrigas en materia de seguridade. As súas actuacións deben ser supervisadas para verificar que se seguen os procedementos establecidos.

2. O persoal relacionado coa información e cos sistemas exercerá e aplicará os principios de seguridade no desempeño da súa función.

3. O significado e alcance do uso seguro do sistema concretarase e plasmarase nunhas normas de seguridade.

4. Para corrixir ou exixir responsabilidades, de ser o caso, cada usuario que acceda á información do sistema debe estar identificado de forma única, de modo que se saiba, en todo momento, quen recibe dereitos de acceso, de que tipo son estes e quen realizou determinada actividade.

Artigo 15. *Profesionalidade.*

1. A seguridade dos sistemas estará atendida, revisada e auditada por persoal cualificado, dedicado e instruído en todas as fases do seu ciclo de vida: instalación, mantemento, xestión de incidencias e desmantelamento.

2. O persoal das administracións públicas recibirá a formación específica necesaria para garantir a seguridade das tecnoloxías da información aplicables aos sistemas e servizos da Administración.

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

Artigo 16. *Autorización e control dos accesos.*

O acceso ao sistema de información deberá ser controlado e limitado aos usuarios, procesos, dispositivos e outros sistemas de información, debidamente autorizados, restrinxindo o acceso ás funcións permitidas.

Artigo 17. *Protección das instalacións.*

Os sistemas instalaranse en áreas separadas, dotadas dun procedemento de control de acceso. Como mínimo, as salas deben estar cerradas e dispor dun control de chaves.

Artigo 18. *Adquisición de produtos de seguridade.*

1. Na adquisición de produtos de seguridade das tecnoloxías da información e comunicacións que vaian utilizar as administracións públicas valoraranse positivamente aqueles que teñan certificada a funcionalidade de seguridade relacionada co obxecto da súa adquisición.
2. A certificación indicada no número anterior deberá estar de acordo coas normas e estándares de maior recoñecemento internacional, no ámbito da seguridade funcional.
3. O Organismo de Certificación do Esquema Nacional de Avaliación e Certificación de Seguridade das Tecnoloxías da Información, constituído ao abeiro do disposto no artigo 2.2.c) do Real decreto 421/2004, do 12 de marzo, e regulado pola Orde PRE/2740/2007, do 19 de setembro, dentro das súas competencias, determinará o criterio que se deberá cumprir en función do uso previsto do produto a que se refira, en relación co nivel de avaliación, outras certificacións de seguridade adicionais que se requiran normativamente, así como, excepcionalmente, nos casos en que non existan produtos certificados. O proceso indicado efectuarase tendo en conta os criterios e as metodoloxías de avaliación, determinados polas normas internacionais que recolle a orde ministerial citada.

Artigo 19. *Seguridade por defecto.*

Os sistemas débense deseñar e configurar de forma que garantan a seguridade por defecto:

a) O sistema proporcionará a mínima funcionalidade requirida para que a organización só alcance os seus obxectivos, e non alcance ningunha outra funcionalidade adicional.
b) As funcións de operación, administración e rexistro de actividade serán as mínimas necesarias, e asegurarase que só son accesibles polas persoas, ou desde lugares ou equipamentos autorizados e poderanse exixir, de ser o caso, restricións de horario e puntos de acceso facultados.
c) Nun sistema de explotación eliminaranse ou desactivaranse, mediante o control da configuración, as funcións que non sexan de interese, sexan innecesarias e, incluso, aquelas que sexan inadecuadas ao fin que se persegue.
d) O uso ordinario do sistema debe ser sinxelo e seguro, de forma que unha utilización insegura requira dun acto consciente por parte do usuario.

Artigo 20. *Integridade e actualización do sistema.*

1. Todo elemento físico ou lóxico requirirá autorización formal previa á súa instalación no sistema.
2. Deberase coñecer en todo momento o estado de seguridade dos sistemas en relación coas especificacións dos fabricantes, coas vulnerabilidades e coas actualizacións que os afecten, e reaccionar con dilixencia para xestionar o risco á vista do seu estado de seguridade.

Artigo 21. *Protección de información almacenada e en tránsito.*

1. Na estrutura e organización da seguridade do sistema, prestaráselle especial atención á información almacenada ou en tránsito a través de contornos inseguros. Terán

a consideración de contornos inseguros os equipamentos portátiles, asistentes persoais (PDA), dispositivos periféricos, soportes de información e comunicacións sobre redes abertas ou con cifrado débil.

2. Forman parte da seguridade os procedementos que aseguren a recuperación e conservación a longo prazo dos documentos electrónicos producidos polas administracións públicas no ámbito das súas competencias.

3. Toda información en soporte non electrónico, que fose causa ou consecuencia directa da información electrónica a que se refire o presente real decreto, deberá estar protexida co mesmo grao de seguridade ca esta. Para iso aplicaranse as medidas que correspondan á natureza do soporte en que se encontren, de conformidade coas normas de aplicación á seguridade destes.

Artigo 22. *Prevención ante outros sistemas de información interconectados.*

O sistema debe protexer o perímetro, en particular, se se conecta a redes públicas. Entenderase por rede pública de comunicacións a rede de comunicacións electrónicas que se utiliza, na súa totalidade ou principalmente, para a prestación de servizos de comunicacións electrónicas dispoñibles para o público, de conformidade coa definición establecida no número 26 do anexo II, da Lei 32/2003, do 3 de novembro, xeral de telecomunicacións. En todo caso, analizaranse os riscos derivados da interconexión do sistema, a través de redes, con outros sistemas, e controlarase o seu punto de unión.

Artigo 23. *Rexistro de actividade.*

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

Artigo 24. *Incidentes de seguridade.*

1. Establecerase un sistema de detección e reacción fronte a código daniño.

2. Rexistraranse os incidentes de seguridade que se produzan e as accións de tratamento que se sigan. Estes rexistros empregaranse para a mellora continua da seguridade do sistema.

Artigo 25. *Continuidade da actividade.*

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

Artigo 26. *Mellora continua do proceso de seguridade.*

O proceso integral de seguridade implantado deberá ser actualizado e mellorado de forma continua. Para iso aplicaranse os criterios e métodos recoñecidos na práctica nacional e internacional relativos a xestión das tecnoloxías da información.

Artigo 27. *Cumprimento de requisitos mínimos.*

1. Para dar cumprimento aos requisitos mínimos establecidos no presente real decreto, as administracións públicas aplicarán as medidas de seguridade indicadas no anexo II, tendo en conta:

a) Os activos que constitúen o sistema.

b) A categoría do sistema, segundo o previsto no artigo 43.
c) As decisións que se adopten para xestionar os riscos identificados.

2. Cando un sistema a que afecte este real decreto manexe datos de carácter persoal, seralle de aplicación o disposto na Lei orgánica 15/1999, do 13 de decembro, e normativa de desenvolvemento, sen prexuízo dos requisitos establecidos no Esquema Nacional de Seguridade.

3. Os medidas a que se refiren os números 1 e 2 terán a condición de mínimos exixibles, e poderán ser ampliados por causa da concorrencia indicada ou do prudente arbitrio do responsable da información, tendo en conta o estado da tecnoloxía, a natureza dos servizos prestados e a información manexada, e os riscos a que están expostos.

Artigo 28. *Infraestruturas e servizos comúns.*

A utilización de infraestruturas e servizos comúns recoñecidos nas administracións públicas facilitará o cumprimento dos principios básicos e os requisitos mínimos exixidos neste real decreto en condicións de mellor eficiencia. Os supostos concretos de utilización destas infraestruturas e servizos comúns serán determinados por cada Administración.

Artigo 29. *Guías de seguridade.*

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.

Artigo 30. *Sistemas de información non afectados.*

As administracións públicas poderán determinar aqueles sistemas de información aos cales non lles sexa de aplicación o disposto neste real decreto por tratarse de sistemas non relacionados co exercicio de dereitos nin co cumprimento de deberes por medios electrónicos nin co acceso por medios electrónicos dos cidadáns á información e ao procedemento administrativo, de acordo co previsto na Lei 11/2007, do 22 de xuño.

CAPÍTULO IV

Comunicacións electrónicas

Artigo 31. *Condicións técnicas de seguridade das comunicacións electrónicas.*

1. As condicións técnicas de seguridade das comunicacións electrónicas no relativo á constancia da transmisión e recepción, das súas datas, do contido íntegro das comunicacións e da identificación fidedigna do remitente e do seu destinatario, segundo o establecido na Lei 11/2007, do 22 de xuño, serán implementadas de acordo co establecido no Esquema Nacional de Seguridade.

2. As comunicacións realizadas nos termos indicados no número anterior terán o valor e a eficacia xurídica que corresponda á súa respectiva natureza, de conformidade coa lexislación que resulte de aplicación.

Artigo 32. *Requirimentos técnicos de notificacións e publicacións electrónicas.*

1. As notificacións e publicacións electrónicas de resolucións e actos administrativos realizaranse de forma que cumpran, de acordo co establecido neste real decreto, as seguintes exixencias técnicas:

a) Aseguren a autenticidade do organismo que o publique.
b) Aseguren a integridade da información publicada.
c) Deixen constancia da data e hora da posta á disposición do interesado da resolución ou acto obxecto de publicación ou notificación, así como do acceso ao seu contido.

d) Aseguren a autenticidade do destinatario da publicación ou notificación.

Artigo 33. *Sinatura electrónica.*

1. Os mecanismos de sinatura electrónica aplicaranse nos termos indicados no anexo II desta norma e de acordo co preceptuado na política de sinatura electrónica e de certificados, segundo se establece no Esquema Nacional de Interoperabilidade.

2. A política de sinatura electrónica e de certificados concretará os procesos de xeración, validación e conservación de sinaturas electrónicas, así como as características e os requisitos exixibles aos sistemas de sinatura electrónica, aos certificados, aos servizos de selaxe de tempo e a outros elementos de soporte das sinaturas, sen prexuízo do previsto no anexo II, que se deberá adaptar a cada circunstancia.

CAPÍTULO V

Auditoría da seguridade

Artigo 34. *Auditoría da seguridade.*

1. Os sistemas de información a que se refire este real decreto serán obxecto dunha auditoría regular ordinaria, polo menos cada dous anos, que verifique o cumprimento dos requirimentos do presente Esquema Nacional de Seguridade.

Con carácter extraordinario, deberase realizar esta auditoría sempre que se produzan modificacións substanciais no sistema de información, que poidan repercutir nas medidas de seguridade requiridas. A realización da auditoría extraordinaria determinará a data de cómputo para o cálculo dos dous anos, establecidos para a realización da seguinte auditoría regular ordinaria, indicados no parágrafo anterior.

2. Esta auditoría realizarase en función da categoría do sistema, determinada segundo o disposto no anexo I e de acordo co previsto no anexo III.

3. No marco do disposto no artigo 39 da Lei 11/2007, do 22 de xuño, a auditoría profundará nos detalles do sistema ata o nivel que considere que proporciona evidencia suficiente e relevante, dentro do alcance establecido para a auditoría.

4. Na realización desta auditoría utilizaranse os criterios, métodos de traballo e de conduta xeralmente recoñecidos, así como a normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. O informe de auditoría deberá ditaminar sobre o grao de cumprimento deste real decreto, identificar as súas deficiencias e suxerir as posibles medidas correctoras ou complementarias 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.

6. Os informes de auditoría serán presentados ao responsable do sistema e ao responsable de seguridade competentes. Estes informes serán analizados por este último, que presentará as súas conclusións ao responsable do sistema para que adopte as medidas correctoras adecuadas.

7. No caso dos sistemas de categoría ALTA, visto o ditame de auditoría, o responsable do sistema poderá acordar a retirada de operación dalgunha información, dalgún servizo ou do sistema na súa totalidade, durante o tempo que coide prudente e ata a satisfacción das modificacións prescritas.

8. Os informes de auditoría poderán ser requiridos polos responsables de cada organización con competencias sobre seguridade das tecnoloxías da información.

CAPÍTULO VI

Estado de seguridade dos sistemas

Artigo 35. *Informe do estado da seguridade.*

O Comité Sectorial de Administración Electrónica articulará os procedementos necesarios para coñecer regularmente o estado das principais variables da seguridade nos sistemas de información a que se refire este real decreto, de forma que permita elaborar un perfil xeral do estado da seguridade nas administracións públicas.

CAPÍTULO VII

Resposta a incidentes de seguridade

Artigo 36. *Capacidade de resposta a incidentes de seguridade da información.*

O Centro Criptolóxico Nacional (CCN) articulará a resposta aos incidentes de seguridade referentes á estrutura denominada CCN-CERT (Centro Criptolóxico Nacional- Computer Emergency Reaction Team), que actuará sen prexuízo das capacidades de resposta a incidentes de seguridade que poida ter cada Administración pública e da función de coordinación a nivel nacional e internacional do CCN.

Artigo 37. *Prestación de servizos de resposta a incidentes de seguridade ás administracións públicas.*

1. De acordo co previsto no artigo 36, o CCN-CERT prestará ás administracións públicas os seguintes servizos:

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 solicitar os informes de auditoría dos sistemas afectados.

b) Investigación e divulgación das mellores prácticas sobre seguridade da información entre todos os membros das administracións públicas. Con esta finalidade, as series de documentos CCN-STIC (Centro Criptolóxico Nacional- Seguridade das Tecnoloxías de Información e Comunicacións), elaboradas polo Centro Criptolóxico Nacional, ofrecerán normas, instrucións, guías e recomendacións para aplicar o Esquema Nacional de Seguridade e para garantir a seguridade dos sistemas de tecnoloxías da información na Administración.

c) Formación destinada ao persoal da Administración especialista no campo da seguridade das tecnoloxías da información, co obxecto de facilitar a actualización de coñecementos do persoal da Administración e de lograr a sensibilización e mellora das súas capacidades para a detección e xestión de incidentes.

d) Información sobre vulnerabilidades, alertas e avisos de novas ameazas aos sistemas de información, recompiladas de diversas fontes de recoñecido prestixio, incluídas as propias.

2. O CCN desenvolverá un programa que ofreza a información, formación, recomendacións e ferramentas necesarias para que as administracións públicas poidan desenvolver as súas propias capacidades de resposta a incidentes de seguridade, e no que aquel será coordinador a nivel público estatal.

CAPÍTULO VIII

Normas de conformidade

Artigo 38. *Sedes e rexistros electrónicos.*

A seguridade das sedes e rexistros electrónicos, así como a do acceso electrónico dos cidadáns aos servizos públicos, rexeranse polo establecido no Esquema Nacional de Seguridade.

Artigo 39. *Ciclo de vida de servizos e sistemas.*

As especificacións de seguridade incluiranse no ciclo de vida dos servizos e sistemas, acompañadas dos correspondentes procedementos de control.

Artigo 40. *Mecanismos de control.*

Cada órgano da Administración pública ou entidade de dereito público establecerá os seus mecanismos de control para garantir de forma real e efectiva o cumprimento do Esquema Nacional de Seguridade.

Artigo 41. *Publicación de conformidade.*

Os órganos e entidades de dereito público darán publicidade nas correspondentes sedes electrónicas ás declaracións de conformidade e aos distintivos de seguridade de que sexan acredores, obtidos respecto ao cumprimento do Esquema Nacional de Seguridade.

CAPÍTULO IX

Actualización

Artigo 42. *Actualización permanente.*

O Esquema Nacional de Seguridade deberase manter actualizado de maneira permanente. Desenvolverase e perfeccionarase ao longo do tempo, en paralelo ao progreso dos servizos de Administración electrónica, da evolución tecnolóxica e novos estándares internacionais sobre seguridade e auditoría nos sistemas e tecnoloxías da información e a medida que se vaian consolidando as infraestruturas que o apoian.

CAPÍTULO X

Categorización dos sistemas de información

Artigo 43. *Categorías.*

1. A categoría dun sistema de información, en materia de seguridade, modulará o equilibrio entre a importancia da información que manexa, os servizos que presta e o esforzo de seguridade requirido, en función dos riscos a que está exposto, baixo o criterio do principio de proporcionalidade.
2. A determinación da categoría indicada no número anterior efectuarase en función da valoración do impacto que tería un incidente que afectar a seguridade da información ou dos servizos con prexuízo para a dispoñibilidade, autenticidade, integridade, confidencialidade ou trazabilidade, como dimensións de seguridade, seguindo o procedemento establecido no anexo I.
3. A valoración das consecuencias dun impacto negativo sobre a seguridade da información e dos servizos efectuarase atendendo á súa repercusión na capacidade da organización para o logro dos seus obxectivos, a protección dos seus activos, o cumprimento das súas obrigas de servizo, o respecto da legalidade e os dereitos dos cidadáns.

Artigo 44. *Facultades.*

1. A facultade para efectuar as valoracións a que se refire o artigo 43, así como a modificación posterior, de ser o caso, corresponderá, dentro do ámbito da súa actividade, ao responsable de cada información ou servizo.

2. A facultade para determinar a categoría do sistema corresponderá ao responsable deste.

Disposición adicional primeira. *Formación.*

O persoal das administracións públicas recibirá, de acordo co previsto na disposición adicional segunda da Lei 11/2007, do 22 de xuño, a formación necesaria para garantir o coñecemento do presente Esquema Nacional de Seguridade, e para este fin os órganos responsables disporán o necesario para que a formación sexa unha realidade efectiva.

Disposición adicional segunda. *Instituto Nacional de Tecnoloxías da Comunicación (INTECO) e organismos análogos.*

O Instituto Nacional de Tecnoloxías da Comunicación (INTECO), como centro de excelencia promovido polo Ministerio de Industria, Turismo e Comercio para o desenvolvemento da sociedade do coñecemento, poderá desenvolver proxectos de innovación e programas de investigación dirixidos á mellor implantación das medidas de seguridade recollidas neste real decreto.

Así mesmo, as administracións públicas poderán dispor de entidades análogas para levar a cabo estas actividades ou outras adicionais no ámbito das súas competencias.

Disposición adicional terceira. *Comité de Seguridade da Información das Administracións Públicas.*

O Comité de Seguridade da Información das Administracións Públicas, dependente do Comité Sectorial de Administración Electrónica, contará cun representante de cada unha das entidades presentes nese comité sectorial. Terá funcións de cooperación en materias comúns relacionadas coa adecuación e implantación do previsto no Esquema Nacional de Seguridade e nas normas, instrucións, guías e recomendacións ditadas para a súa aplicación.

Disposición adicional cuarta. Modificación do Regulamento de desenvolvemento da Lei orgánica 15/1999, de protección de datos de carácter persoal, aprobado polo Real decreto 1720/2007, do 21 de decembro.

Modifícase a letra b) do número 5 do artigo 81 do Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal, aprobado polo Real decreto 1720/2007, do 21 de decembro, que pasa a ter a seguinte redacción:

«b) Se trate de ficheiros ou tratamentos en que de forma incidental ou accesoria se conteñan aqueles datos sen gardar relación coa súa finalidade.»

Disposición transitoria. *Adecuación de sistemas.*

1. Os sistemas existentes no momento da entrada en vigor deste real decreto adecuaranse ao Esquema Nacional de Seguridade de forma que permitan o cumprimento do establecido na disposición derradeira terceira da Lei 11/2007, do 22 de xuño. Os novos sistemas aplicarán o establecido neste real decreto desde a súa concepción.

2. Se aos doce meses da entrada en vigor do Esquema Nacional de Seguridade houber circunstancias que impidan a plena aplicación do exixido nel, disporase dun plan de adecuación que marque os prazos de execución os cales, en ningún caso, serán superiores a 48 meses desde a entrada en vigor.

O plan indicado no número anterior será elaborado coa antelación suficiente e aprobado polos órganos superiores competentes.

3. Mentres o órgano superior competente non aprobe unha política de seguridade serán de aplicación as políticas de seguridade que poidan existir a nivel de órgano directivo.

Disposición derrogatoria única.

Quedan derrogadas as disposicións de igual ou inferior rango que se opoñan ao disposto neste regulamento.

Disposición derradeira primeira. *Título habilitante.*

Este real decreto dítase en virtude do establecido no artigo 149.1.18ª da Constitución, que lle atribúe ao Estado a competencia sobre as bases do réxime xurídico das administracións públicas.

Disposición derradeira segunda. *Desenvolvemento normativo.*

Autorízase o titular do Ministerio da Presidencia para ditar as disposicións necesarias para a aplicación e o desenvolvemento do establecido neste real decreto, sen prexuízo das competencias das comunidades autónomas de desenvolvemento e execución da lexislación básica do Estado.

Disposición derradeira terceira. *Entrada en vigor.*

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

Dado en Madrid o 8 de xaneiro de 2010.

JUAN CARLOS R.

A vicepresidenta primeira e ministra da Presidencia
María Teresa Fernández de la Vega Sanz.

ANEXOS

ANEXO I

Categorías dos sistemas

1. Fundamentos para a determinación da categoría dun sistema.

A determinación da categoría dun sistema baséase na valoración do impacto que tería sobre a organización un incidente que afecte a seguridade da información ou dos sistemas, con repercusión na capacidade organizativa para:

a) Alcanzar os seus obxectivos.
b) Protexer os activos ao seu cargo.
c) Cumprir as súas obrigas diarias de servizo.
d) Respectar a legalidade vixente.
e) Respectar os dereitos das persoas.

A determinación da categoría dun sistema realizarase de acordo co establecido neste real decreto e será de aplicación a todos os sistemas empregados para a prestación dos servizos da Administración electrónica e soporte do procedemento administrativo xeral.

2. Dimensións da seguridade.

Co fin de poder determinar o impacto que tería sobre a organización un incidente que afecte a seguridade da información ou dos sistemas, e de poder establecer a categoría do sistema, teranse en conta as seguintes dimensións da seguridade, que serán identificadas polas súas correspondentes iniciais en maiúsculas:

a) Dispoñibilidade [D].
b) Autenticidade [A].
c) Integridade [I].
d) Confidencialidade [C].
e) Trazabilidade [T].

3. Determinación do nivel requirido nunha dimensión de seguridade.

Unha información ou un servizo pódense ver afectados nunha ou máis das súas dimensións de seguridade. Cada dimensión de seguridade afectada adscribirase a un dos seguintes niveis: BAIXO, MEDIO ou ALTO. Se unha dimensión de seguridade non se ve afectada, non se adscribirá a ningún nivel.

a) Nivel BAIXO. Utilizarase cando as consecuencias dun incidente de seguridade que afecte algunha das dimensións de seguridade supoñan un prexuízo limitado sobre as funcións da organización, sobre os seus activos ou sobre os individuos afectados.
Entenderase por prexuízo limitado:

1º. A redución de forma apreciable da capacidade da organización para atender eficazmente as súas obrigas correntes, aínda que estas se sigan desempeñando.
2º. O sufrimento dun dano menor polos activos da organización.
3º. O incumprimento formal dalgunha lei ou regulación, que teña carácter de emendable.
4º. Causar un prexuízo menor a algún individuo que, mesmo sendo molesto, poida ser facilmente reparable.
5º. Outros de natureza análoga.

b) Nivel MEDIO. Utilizarase cando as consecuencias dun incidente de seguridade que afecte algunha das dimensións de seguridade supoñan un prexuízo grave sobre as funcións da organización, sobre os seus activos ou sobre os individuos afectados.

Entenderase por prexuízo grave:

1º. A redución significativa da capacidade da organización para atender eficazmente as súas obrigas fundamentais, aínda que estas se sigan desempeñando.
2º. O sufrimento dun dano significativo polos activos da organización.
3º. O incumprimento material dalgunha lei ou regulación, ou o incumprimento formal que non teña carácter de emendable.
4º. Causar un prexuízo significativo a algún individuo, de difícil reparación.
5º. Outros de natureza análoga.

c) Nivel ALTO. Utilizarase cando as consecuencias dun incidente de seguridade que afecte algunha das dimensións de seguridade supoñan un prexuízo moi grave sobre as funcións da organización, sobre os seus activos ou sobre os individuos afectados.
Entenderase por prexuízo moi grave:

1º. A anulación da capacidade da organización para atender algunha das súas obrigas fundamentais e que estas se sigan desempeñando.
2º. O sufrimento dun dano moi grave, e incluso irreparable, polos activos da organización.
3º. O incumprimento grave dalgunha lei ou regulación.
4º. Causar un prexuízo grave a algún individuo, de difícil ou imposible reparación.
5º. Outros de natureza análoga.

Cando un sistema manexe diferentes informacións e preste diferentes servizos, o nivel do sistema en cada dimensión será o maior dos establecidos para cada información e cada servizo.

4. Determinación da categoría dun sistema de información.

1. Defínense tres categorías: BÁSICA, MEDIA e ALTA.

a) Un sistema de información será de categoría ALTA se algunha das súas dimensións de seguridade alcanza o nivel ALTO.
b) Un sistema de información será de categoría MEDIA se algunha das súas dimensións de seguridade alcanza o nivel MEDIO, e ningunha alcanza un nivel superior.
c) Un sistema de información será de categoría BÁSICA se algunha das súas dimensións de seguridade alcanza o nivel BAIXO, e ningunha alcanza un nivel superior.

2. A determinación da categoría dun sistema sobre a base do indicado no número anterior non implicará que se altere, por este feito, o nivel das dimensións de seguridade que non influíron na determinación da súa categoría.

5. Secuencia de actuacións para determinar a categoría dun sistema:

1. Identificación do nivel correspondente a cada información e servizo, en función das dimensións de seguridade, tendo en conta o establecido no número 3.
2. Determinación da categoría do sistema, segundo o establecido no número 4.

ANEXO II

1. Disposicións xerais

1. Para lograr o cumprimento dos principios básicos e requisitos mínimos establecidos aplicaranse as medidas de seguridade indicadas neste anexo, as cales serán proporcionais:

a) Ás dimensións de seguridade relevantes no sistema que se vaia protexer.
b) Á categoría do sistema de información que se vaia protexer.

2. As medidas de seguridade divídense en tres grupos:

a) Marco organizativo [org]. Constituído polo conxunto de medidas relacionadas coa organización global da seguridade.
b) Marco operacional [op]. Formado polas medidas que se tomarán para protexer a operación do sistema como conxunto integral de compoñentes para un fin.
c) Medidas de protección [mp]. Céntranse en protexer activos concretos, segundo a súa natureza e a calidade exixida polo nivel de seguridade das dimensións afectadas.

2. Selección de medidas de seguridade

1. Para a selección das medidas de seguridade seguiranse os pasos seguintes:

a) Identificación dos tipos de activos presentes.
b) Determinación das dimensións de seguridade relevantes, tendo en conta o establecido no anexo I.
c) Determinación do nivel correspondente a cada dimensión de seguridade, tendo en conta o establecido no anexo I.
d) Determinación da categoría do sistema, segundo o establecido no anexo I.
e) Selección das medidas de seguridade apropiadas de entre as contidas neste anexo, de acordo coas dimensións de seguridade e cos seus niveis e, para determinadas medidas de seguridade, de acordo coa categoría do sistema.

2. Para os efectos de facilitar o cumprimento do disposto neste anexo, cando nun sistema de información existan sistemas que requiran a aplicación dun nivel de medidas de seguridade diferente ao do sistema principal, poderanse segregar deste último, e será de aplicación en cada caso o nivel de medidas de seguridade correspondente e sempre que se poidan delimitar a información e os servizos afectados.
3. A relación de medidas seleccionadas formalizarase nun documento denominado declaración de aplicabilidade, asinado polo responsable da seguridade do sistema.
4. A correspondencia entre os niveis de seguridade exixidos en cada dimensión e as medidas de seguridade é a que se indica na táboa seguinte:

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	n.a.	+	++	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
categoría	n.a.	aplica	=	op.exp.7	Xestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Rexistro da actividade dos usuarios
categoría	n.a.	aplica	=	op.exp.9	Rexistro da xestión de incidencias
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.	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 equipamento
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 obrigas
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	n.a.	aplica	=	mp.si.5	Borrado e destrución
				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	Cifrado
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	n.a.	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

Nas táboas deste anexo empréganse as seguintes convencións:

a) Para indicar que unha determinada medida de seguridade se debe aplicar a unha ou varias dimensións de seguridade nalgún nivel determinado utilízase a voz «aplica».

b) «n.a.» significa «non aplica».

c) Para indicar que as exixencias dun nivel son iguais ás do nivel inferior utilízase o signo «=».

d) Para indicar o incremento de exixencias graduado en función do nivel da dimensión de seguridade, utilízanse os signos «+» e «++».

e) Para indicar que unha medida protexe especificamente unha certa dimensión de seguridade, esta explicítase mediante a súa inicial.

3. **Marco organizativo [org]**

O marco organizativo está constituído por un conxunto de medidas relacionadas coa organización global da seguridade.

3.1 Política de seguridade [org.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

A política de seguridade será aprobada polo órgano superior competente que corresponda, de acordo co establecido no artigo 11, e plasmarase nun documento escrito en que, de forma clara, se precise, polo menos, o seguinte:

a) Os obxectivos ou misión da organización.

b) O marco legal e regulatorio en que se desenvolverán as actividades.

c) Os roles ou funcións de seguridade, definindo para cada un os deberes e as responsabilidades do cargo, así como o procedemento para a súa designación e renovación.

d) A estrutura do comité ou os comités para a xestión e coordinación da seguridade, detallando o seu ámbito de responsabilidade, os membros e a relación con outros elementos da organización.

e) As directrices para a estruturación da documentación de seguridade do sistema, a súa xestión e o acceso.

A política de seguridade debe referenciar e ser coherente co establecido no documento de seguridade que exixe o Real decreto 1720/2007, no que corresponda.

3.2 Normativa de seguridade [org.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Disporase dunha serie de documentos que describan:

a) O uso correcto de equipamentos, servizos e instalacións.

b) O que se considerará uso indebido.

c) A responsabilidade do persoal con respecto ao cumprimento ou violación destas normas: dereitos, deberes e medidas disciplinarias de acordo coa lexislación vixente.

3.3 Procedementos de seguridade [org.3].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Disporase dunha serie de documentos que detallen de forma clara e precisa:

a) Como levar a cabo as tarefas habituais.

b) Quen debe facer cada tarefa.

c) Como identificar e reportar comportamentos anómalos.

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 enlaces 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.

4 Marco operacional [op]

O marco operacional está constituído polas medidas que se deben tomar para protexer a operación do sistema como conxunto integral de compoñentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análise de riscos [op.pl.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Bastará unha análise informal, realizada en linguaxe natural. É dicir, unha exposición textual que describa os seguintes aspectos:

a) Identifique os activos máis valiosos do sistema.
b) Identifique as ameazas máis probables.
c) Identifique as salvagardas que protexen desas ameazas.
d) Identifique os principais riscos residuais.

Categoría MEDIA

Deberase realizar unha análise semi-formal, usando unha linguaxe específica, cun catálogo básico de ameazas e unha semántica definida. É dicir, unha presentación con táboas que describa os seguintes aspectos:

a) Identifique e valore cualitativamente os activos máis valiosos do sistema.
b) Identifique e cuantifique as ameazas máis probables.
c) Identifique e valore as salvagardas que protexen desas ameazas.
d) Identifique e valore o risco residual.

Categoría ALTA

Deberase realizar unha análise formal, usando unha linguaxe específica, cun fundamento matemático recoñecido internacionalmente. A análise deberá cubrir os seguintes aspectos:

a) Identifique e valore cualitativamente os activos máis valiosos do sistema.
b) Identifique e cuantifique as ameazas posibles.
c) Identifique as vulnerabilidades habilitantes desas ameazas.
d) Identifique e valore as salvagardas adecuadas.
e) Identifique e valore o risco residual.

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

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

A seguridade do sistema será obxecto dunha proposta integral detallando, polo menos, os seguintes aspectos:

a) Documentación das instalacións:

1.º Áreas.
2.º Puntos de acceso.

b) Documentación do sistema:

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

c) Esquema de liñas de defensa:

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

d) Sistema de identificación e autenticación de usuarios:

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

e) Controis técnicos internos:

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

f) Sistema de xestión con actualización e aprobación periódica.

4.1.3 Adquisición de novos compoñentes [op.pl.3].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

Establecerase un proceso formal para planificar a adquisición de novos compoñentes do sistema, proceso que:

a) Atenderá as conclusións da análise de riscos: [op.pl.1].
b) Será acorde coa arquitectura de seguridade escollida: [op.pl.2].
c) Terá en conta as necesidades técnicas, de formación e de financiamento de forma conxunta.

4.1.4 Dimensionamento / xestión de capacidades [op.pl.4].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	aplica	=

Con carácter previo á posta en explotación, realizarase un estudo previo que cubrirá os seguintes aspectos:

a) Necesidades de procesamento.
b) Necesidades de almacenamento de información: durante o seu procesamento e durante o período que se deba reter.
d) Necesidades de comunicación.
e) Necesidades de persoal: cantidade e cualificación profesional.
f) Necesidades de instalacións e medios auxiliares.

4.1.5 Compoñentes certificados [op.pl.5].

dimensións	todas		
categoría	básica	media	alta
	non aplica	no aplica	aplica

Utilizaranse preferentemente sistemas, produtos ou equipamentos cuxas funcionalidades de seguridade e o seu nivel fosen avaliados conforme normas europeas ou internacionais e que estean certificados por entidades independentes de recoñecida solvencia.

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

Terán a consideración de entidades independentes de recoñecida solvencia as recollidas nos acordos ou arranxos internacionais de recoñecemento mutuo dos certificados da seguridade da tecnoloxía da información ou outras de natureza análoga.

4.2 Control de acceso. [op.acc].

O control de acceso cobre o conxunto de actividades preparatorias e executivas para que unha determinada entidade, usuario ou proceso, poida, ou non, acceder a un recurso do sistema para realizar unha determinada acción.

O control de acceso que se implante nun sistema real será un punto de equilibrio entre a comodidade de uso e a protección da información. En sistemas de nivel baixo primarase a comodidade, mentres que en sistemas de nivel alto se primará a protección.

En todo control de acceso se requirirá o seguinte:

a) Que todo acceso estea prohibido, salvo concesión expresa.
b) Que a entidade quede identificada singularmente [op.acc.1].
c) Que a utilización dos recursos estea protexida [op.acc.2].
d) Que se definan para cada entidade os seguintes parámetros: a qué se necesita acceder, con que dereitos e baixo que autorización [op.acc.4].
e) Serán diferentes as persoas que autorizan, usan e controlan o uso [op.acc.3].
f) Que a identidade da entidade quede suficientemente autenticada [mp.acc.5].
g) Que se controle tanto o acceso local ([op.acc.6]) coma o acceso remoto ([op.acc.7]).

Co cumprimento de todas as medidas indicadas garantirase que ninguén accederá a recursos sen autorización. Ademais, quedará rexistrado o uso do sistema ([op.exp.8]) para poder detectar e reaccionar ante calquera fallo accidental ou deliberado.

Cando se interconecten sistemas nos cales a identificación, autenticación e autorización teñan lugar en diferentes dominios de seguridade, baixo distintas responsabilidades, nos casos en que sexa necesario, as medidas de seguridade locais acompañaranse dos correspondentes acordos de colaboración que delimiten mecanismos e procedementos para a atribución e exercicio efectivos das responsabilidades de cada sistema ([op.ext]).

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 continuación:

a) Asignarase un identificador singular para cada entidade (usuario ou proceso) que accede ao sistema, de tal forma que:

1.º Se pode saber quen recibe e que dereitos de acceso recibe.
2.º Se pode saber quen fixo algo e que fixo.

b) As contas de usuario xestionaranse da seguinte forma:

1.º Cada conta estará asociada a un identificador único.
2.º 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 sentido contrario.
3.º As contas reteranse durante o período necesario para atender as necesidades de trazabilidade dos rexistros de actividade asociados a elas. Este período será denominado período de retención.

4.2.2 Requisitos de acceso [op.acc.2].

dimensións	I C A T		
nivel	baixo	medio	alto
	aplica	=	=

Os requisitos de acceso ateranse ao que a continuación se indica:

a) Os recursos do sistema protexeranse con algún mecanismo que impida a súa utilización, salvo ás entidades que desfruten de dereitos de acceso suficientes.
b) Os dereitos de acceso de cada recurso estableceranse segundo as decisións da persoa responsable do recurso e observarán a política e normativa de seguridade do sistema.
c) Particularmente se controlará o acceso aos compoñentes do sistema e aos seus ficheiros ou rexistros de configuración.

4.2.3 Segregación de funcións e tarefas [op.acc.3].

dimensións	I C A T		
nivel	bajo	medio	alto
	non aplica	aplica	=

O sistema de control de acceso organizarase de forma que se exixa a concorrencia de dúas ou máis persoas para realizar tarefas críticas, anulando a posibilidade de que un só individuo autorizado poida abusar dos seus dereitos para cometer algunha acción ilícita.
En concreto, separaranse polo menos as seguintes funcións:

a) Desenvolvemento de operación.
b) Configuración e mantemento do sistema de operación.
c) Auditoría ou supervisión de calquera outra función.

4.2.4 Proceso de xestión de dereitos de acceso [op.acc.4].

dimensións	I C A T		
nivel	baixo	medio	alto
	aplica	=	=

Os dereitos de acceso de cada usuario limitaranse atendendo aos seguintes principios:

a) Mínimo privilexio. Os privilexios de cada usuario reduciranse ao mínimo estritamente necesario para cumprir as súas obrigas. Desta forma acóutanse os danos que puider causar unha entidade, de forma accidental ou intencionada.
b) Necesidade de coñecer. Os privilexios limitaranse de forma que os usuarios só accederán ao coñecemento daquela información requirida para cumprir as súas obrigas.
c) Capacidade de autorizar. Só e exclusivamente o persoal con competencia poderá conceder, alterar ou anular a autorización de acceso aos recursos, conforme os criterios establecidos polo seu propietario.

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

dimensións	I C A T		
nivel	baixo	medio	alto
	aplica	+	++

Os mecanismos de autenticación fronte ao sistema adecuaranse ao nivel do sistema atendendo ás consideracións que seguen.
As guías CCN-STIC desenvolverán os mecanismos concretos adecuados a cada nivel.

Nivel BAIXO

a) Admitirase o uso de calquera mecanismo de autenticación: claves concertadas ou dispositivos físicos (en expresión inglesa «tokens») ou compoñentes lóxicos tales como certificados software ou outros equivalentes ou mecanismos biométricos.
b) No caso de usar contrasinais aplicaranse regras básicas de calidade destas.
c) Atenderase á seguridade dos autenticadores de forma que:

1.º Os autenticadores se activarán unha vez que estean baixo o control efectivo do usuario.
2.º Os autenticadores estarán baixo o control exclusivo do usuario.
3.º O usuario recoñecerá que os recibiu e que coñece e acepta as obrigas que implica a súa tenza, en particular o deber de custodia dilixente, protección da súa confidencialidade e información inmediata en caso de perda.
4.º Os autenticadores se cambiarán cunha periodicidade marcada pola política da organización, atendendo á categoría do sistema a que se accede.
5.º Os autenticadores se retirarán e serán deshabilitados cando a entidade (persoa, equipamento ou proceso) que autentican termina a súa relación co sistema.

Nivel MEDIO

a) Non se recomendará o uso de claves concertadas.
b) Recomendarase o uso doutro tipo de mecanismos do tipo dispositivos físicos (tokens) ou compoñentes lóxicos tales como certificados software ou outros equivalentes ou biométricos.
c) No caso de usar contrasinais aplicaranse políticas rigorosas de calidade do contrasinal e renovación frecuente.

Nivel ALTO

a) Os autenticadores suspenderanse tras un período definido de non utilización.
b) Non se admitirá o uso de claves concertadas.
c) Exixirase o uso de dispositivos físicos (tokens) personalizados ou biometría.

d) No caso de utilización de dispositivos físicos (tokens) empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.

e) Empregaranse, preferentemente, produtos certificados [op.pl.5].

Táboa resumo de mecanismos de autenticación admisibles

		Nivel		
		BAIXO	MEDIO	ALTO
algo que se sabe	claves concertadas	si	Con cautela	non
algo que se ten	Tokens	si	si	criptográficos
algo que se é	Biometría	si	si	+ dobre factor

4.2.6 Acceso local [op.acc.6].

dimensións	I C A T		
nivel	baixo	medio	alto
	aplica	+	++

Considérase acceso local o realizado desde postos de traballo dentro das propias instalacións da organización. Estes accesos terán en conta o nivel das dimensións de seguridade:

Nivel BAIXO

a) Previranse ataques que poidan revelar información do sistema sen chegar a acceder a el. A información revelada a quen intenta acceder debe ser a mínima imprescindible (os diálogos de acceso proporcionarán soamente a información indispensable).

b) O número de intentos permitidos será limitado. Bloquearase a oportunidade de acceso unha vez efectuados un certo número de fallos consecutivos.

c) Rexistraranse os accesos con éxito e os fallados.

d) O sistema informará o usuario das súas obrigas inmediatamente despois de obter o acceso.

Nivel MEDIO

Informarase o usuario do último acceso efectuado coa súa identidade.

Nivel ALTO

a) O acceso estará limitado por horario, datas e lugar desde onde se accede.

b) Definiranse aqueles puntos en que o sistema requirirá unha renovación da autenticación do usuario, mediante identificación singular, non bastando coa sesión establecida.

4.2.7 Acceso remoto [op.acc.7].

dimensións	I C A T		
nivel	baixo	medio	alto
	aplica	+	=

Considérase acceso remoto o realizado desde fóra das propias instalacións da organización, a través de redes de terceiros.

Garantirase a seguridade do sistema cando accedan remotamente usuarios ou outras entidades, o que implicará protexer tanto o acceso en si mesmo (como [op.acc.6]) como a canle de acceso remoto (como en [mp.com.2] e [mp.com.3]).

Nivel MEDIO

Establecerase unha política específica do que se pode facer remotamente, e requirirase autorización positiva.

4.3 Explotación [op.exp]

4.3.1 Inventario de activos [op.exp.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Manterase un inventario actualizado de todos os elementos do sistema, detallando a súa natureza e identificando o seu propietario; é dicir, a persoa que é responsable das decisións relativas a el.

4.3.2 Configuración de seguridade [op.exp.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Configuraranse os equipamentos previamente á súa entrada en operación, de forma que:

a) Se retiren contas e contrasinais estándar.
b) Se aplicará a regra de «mínima funcionalidade»:

1.º O sistema debe proporcionar a funcionalidade requirida para que a organización alcance os seus obxectivos e ningunha outra funcionalidade,
2.º Non proporcionará funcións gratuítas, nin de operación, nin de administración, nin de auditoría, reducindo desta forma o seu perímetro ao mínimo imprescindible.
3.º Eliminaranse ou desactivaranse mediante o control da configuración aquelas funcións que non sexan de interese, non sexan necesarias e mesmo aquelas que sexan inadecuadas ao fin que se persegue.

c) Aplicarase a regra de «seguridade por defecto»:

1.º As medidas de seguridade serán respectuosas co usuario e protexerano, salvo que se expoña conscientemente a un risco.
2.º Para reducir a seguridade, o usuario ten que realizar accións conscientes.
3.º O uso natural, nos casos en que o usuario non consultou o manual, será un uso seguro.

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

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

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

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

4.3.4 Mantemento [op.exp.4].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

Para manter o equipamento físico e lóxico que constitúe o sistema aplicarase o seguinte:

a) Atenderase ás especificacións dos fabricantes no relativo a instalación e mantemento dos sistemas.
b) Efectuarase un seguimento continuo dos anuncios de defectos.
c) Disporase dun procedemento para analizar, priorizar e determinar cando aplicar as actualizacións de seguridade, parches, melloras e novas versións. A priorización terá en conta a variación do risco en función da aplicación ou non da actualización.

4.3.5 Xestión de cambios [op.exp.5].

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

Manterase un control continuo de cambios realizados no sistema, de forma que:

a) Todos os cambios anunciados polo fabricante ou provedor serán analizados para determinar a súa conveniencia para seren incorporados, ou non.
b) Antes de pór en produción unha nova versión ou unha versión parcheada comprobarase, nun equipamento que non estea en produción, que a nova instalación funciona correctamente e non diminúe a eficacia das funcións necesarias para o traballo diario. O equipamento de probas será equivalente ao de produción nos aspectos que se comproban.
c) Os cambios se planificarán para reducir o impacto sobre a prestación dos servizos afectados.
d) Mediante análise de riscos determinarase se os cambios son relevantes para a seguridade do sistema. Aqueles cambios que impliquen unha situación de risco de nivel alto serán aprobados explicitamente de forma previa á súa implantación.

4.3.6 Protección fronte a código daniño [op.exp.6].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

Considérase código daniño: os virus, os vermes, os troianos, os programas espías, coñecidos en terminoloxía inglesa como «spyware» e, en xeral, todo o coñecido como «malware».

Disporase de mecanismos de prevención e reacción fronte a código daniño con mantemento de acordo coas recomendacións do fabricante.

4.3.7 Xestión de incidencias [op.exp.7].

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

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

a) Procedemento de reporte de incidentes reais ou sospeitosos, detallando o escalado da notificación.

b) Procedemento de toma de medidas urxentes, incluíndo a detención de servizos, o illamento do sistema afectado, a recollida de evidencias e 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.º Previr que se repita o incidente.

2.º Incluír nos procedementos de usuario a identificación e forma de tratar o incidente.

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

A xestión de incidentes que afecten datos de carácter persoal terá en conta o disposto no Real decreto 1720 de 2007, no que corresponda.

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

dimensións	T		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Rexistraranse todas as actividades dos usuarios no sistema, de forma que:

a) O rexistro indicará quen realiza a actividade, cando a realiza e sobre que información.

b) Se incluirá a actividade dos usuarios e, especialmente, a dos operadores e administradores do sistema en canto poden acceder á configuración e actuar no seu mantemento.

c) Se deben rexistrar as actividades realizadas con éxito e os intentos fracasados.

d) A determinación de que actividades se deben rexistrar e con que niveis de detalle determinarase á vista da análise de riscos realizada sobre o sistema ([op.pl.1]).

4.3.9 Rexistro da xestión de incidencias [op.exp.9].

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

Rexistraranse todas as actuacións relacionadas coa xestión de incidencias, de forma que:

a) Se rexistrarán o reporte inicial, as actuacións de emerxencia e as modificacións do sistema derivadas do incidente.
b) Se rexistrará aquela evidencia que poida, posteriormente, sustentar unha demanda xudicial, ou facer fronte a ela, cando o incidente poida levar a actuacións disciplinarias sobre o persoal interno, sobre provedores externos ou á persecución de delitos. Na determinación da composición e detalle destas evidencias recorrerase a asesoramento legal especializado.
c) Como consecuencia da análise das incidencias, revisarase a determinación dos eventos auditables.

4.3.10 Protección dos rexistros de actividade [op.exp.10].

dimensións	T		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Protexeranse os rexistros do sistema, de forma que:

a) Se determinará o período de retención dos rexistros.
b) Se asegurará a data e hora. Véxase [mp.info.5].
c) Os rexistros non poderán ser modificados nin eliminados por persoal non autorizado.
d) As copias de seguridade, se existen, axustaranse aos mesmos requisitos.

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) arquivo 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.
b) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.

4.4 Servizos externos [op.ext]

Cando se utilicen recursos externos á organización, sexan servizos, equipamentos, instalacións ou persoal, deberase ter en conta que a delegación se limita ás funcións.

A organización segue sendo en todo momento responsable dos riscos en que se incorre na medida en que impacten sobre a información manexada e os servizos finais prestados pola organización.

A organización disporá as medidas necesarias para poder exercer a súa responsabilidade e manter o control en todo momento.

4.4.1 Contratación e acordos de nivel de servizo [op.ext.1]

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

Previamente á utilización de recursos externos estableceranse contractualmente as características do servizo prestado e as responsabilidades das partes. Detallarase o que se considera calidade mínima do servizo prestado e as consecuencias do seu incumprimento.

4.4.2 Xestión diaria [op.ext.2].

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

Para a xestión diaria do sistema, estableceranse os seguintes puntos:

a) Un sistema rutineiro para medir o cumprimento das obrigas 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 incidencias e desastres (véxase [op.exp.7]).

4.4.3 Medios alternativos [op.ext.9].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Estará prevista a provisión do servizo por medios alternativos en caso de indispoñibilidade do servizo contratado. O servizo alternativo desfrutará das mesmas garantías de seguridade que o servizo habitual.

4.5 Continuidade do servizo [op.cont]

4.5.1 Análise de impacto [op.cont.1].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	aplica	=

Realizarase unha análise de impacto que permita determinar:

a) Os requisitos de dispoñibilidade de cada servizo medidos como o impacto dunha interrupción durante un certo período de tempo.
b) Os elementos que son críticos para a prestación de cada servizo.

4.5.2 Plan de continuidade [op.cont.2].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Desenvolverase un plan de continuidade que estableza as accións que se deberán executar en caso de interrupción dos servizos prestados cos medios habituais. Este plan incluirá os seguintes aspectos:

a) Identificaranse funcións, responsabilidades e actividades que se van realizar.
b) Existirá unha previsión dos medios alternativos que se vai conxugar para poder seguir prestando os servizos.
c) Todos os medios alternativos estarán planificados e materializados en acordos ou contratos cos provedores correspondentes.
d) As persoas afectadas polo plan recibirán formación específica relativa ao seu papel no citado plan.
e) O plan de continuidade será parte integral e harmónica dos plans de continuidade da organización noutras materias alleas á seguridade.

4.5.3 Probas periódicas [op.cont.3].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Realizaranse probas periódicas para localizar e corrixir, de ser o caso, os erros ou deficiencias que poidan existir no plan de continuidade.

4.6 Monitorización do sistema [op.mon]

O sistema estará suxeito a medidas de monitorización da súa actividade.

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

dimensións	todas		
categoría	básica	media	alta
	non aplica	non aplica	aplica

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
	non aplica	non aplica	aplica

Establecerase un conxunto de indicadores que mida o desempeño real do sistema en materia de seguridade, nos seguintes aspectos:

a) Grao de implantación das medidas de seguridade.
b) Eficacia e eficiencia das medidas de seguridade.
c) Impacto dos incidentes de seguridade.

5. **Medidas de protección [mp]**

As medidas de protección centraranse en protexer activos concretos, segundo a súa natureza, co nivel requirido en cada dimensión de seguridade.

5.1 Protección das instalacións e infraestruturas [mp.if]

5.1.1 Áreas separadas e con control de acceso [mp.if.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

O equipamento instalarase en áreas separadas específicas para a súa función.
Controlaranse os accesos ás áreas indicadas de forma que só se poida acceder polas entradas previstas e vixiadas.

5.1.2 Identificación das persoas [mp.if.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

O mecanismo de control de acceso aterase ao que se dispón a continuación:

a) Identificaranse todas as persoas que accedan aos locais onde hai equipamento que forme parte do sistema de información.
b) Rexistraranse as entradas e saídas de persoas.

5.1.3 Acondicionamento dos locais [mp.if.3].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Os locais onde se sitúen os sistemas de información e os seus compoñentes disporán de elementos adecuados para o eficaz funcionamento do equipamento alí instalado. E, en especial:

a) Condicións de temperatura e humidade.
b) Protección fronte ás ameazas identificadas na análise de riscos.
c) Protección do cableado fronte a incidentes fortuítos ou deliberados.

5.1.4 Enerxía eléctrica [mp.if.4].

dimensións	D		
nivel	baixo	medio	alto
	aplica	+	=

Os locais onde se sitúen os sistemas de información e os seus compoñentes disporán da enerxía eléctrica, e as súas tomas correspondentes, necesaria para o seu funcionamento, de forma que neles:

a) Se garantirá a subministración de potencia eléctrica.
b) Se garantirá o correcto funcionamento das luces de emerxencia.

Nivel MEDIO

Garantirase a subministración eléctrica aos sistemas en caso de fallo da subministración xeral, garantindo o tempo suficiente para unha terminación ordenada dos procesos, salvagardando a información.

5.1.5 Protección fronte a incendios [mp.if.5].

dimensións	D		
nivel	baixo	medio	alto
	aplica	=	=

Os locais onde se sitúen os sistemas de información e os seus compoñentes protexeranse fronte a incendios fortuítos ou deliberados, aplicando polo menos a normativa industrial pertinente.

5.1.6 Protección fronte a inundacións [mp.if.6].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	aplica	=

Os locais onde se sitúen os sistemas de información e os seus compoñentes protexeranse fronte a incidentes fortuítos ou deliberados causados pola auga.

5.1.7 Rexistro de entrada e saída de equipamento [mp.if.7].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Levarase un rexistro pormenorizado de toda entrada e saída de equipamento, incluíndo a identificación da persoa que autoriza de movemento.

5.1.8 Instalacións alternativas [mp.if.9].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Garantirase a existencia e dispoñibilidade de instalacións alternativas para poder traballar en caso de que as instalacións habituais non estean dispoñibles. As instalacións alternativas desfrutarán das mesmas garantías de seguridade que as instalacións habituais.

5.2 Xestión do persoal [mp.per].

5.2.1 Caracterización do posto de traballo [mp.per.1].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	aplica	=

Cada posto de traballo caracterizarase da seguinte forma:

a) Definiranse as responsabilidades relacionadas con cada posto de traballo en materia de seguridade. A definición basearase na análise de riscos.
b) Definiranse os requisitos que deben satisfacer as persoas que vaian ocupar o posto de traballo, en particular, en termos de confidencialidade.
c) Estes requisitos teranse en conta na selección da persoa que vaia ocupar ese posto, incluíndo a verificación dos seus antecedentes laborais, formación e outras referencias.

5.2.2 Deberes e obrigas [mp.per.2].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

1. Informarase a cada persoa que traballe no sistema dos deberes e responsabilidades do seu posto de traballo en materia de seguridade.

a) Especificaranse as medidas disciplinarias que procedan.
b) Cubrirase tanto o período durante o cal se desempeña o posto como as obrigas en caso de termo da asignación, ou traslado a outro posto de traballo.
c) Considerarase o deber de confidencialidade respecto dos datos a que teña acceso, tanto durante o período que estean adscritos ao posto de traballo como posteriormente á súa terminación.

2. En caso de persoal contratado a través dun terceiro:

a) Estableceranse os deberes e obrigas do persoal.
b) Estableceranse os deberes e obrigas de cada parte.
c) Establecerase o procedemento de resolución de incidentes relacionados co incumprimento das obrigas.

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 incidencias de seguridade, sexan reais ou falsas alarmas.

5.2.4 Formación [mp.per.4].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	=

Formarase regularmente o persoal naquelas materias que requiran para o desempeño das súas funcións, en particular no relativo a:

a) Configuración de sistemas.
b) Detección e reacción a incidentes.
c) Xestión da información en calquera soporte en que se encontre. Cubriranse polo menos as seguintes actividades: almacenamento, transferencia, copias, distribución e destrución.

5.2.5 Persoal alternativo [mp.per.9].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Garantirase a existencia e dispoñibilidade doutras persoas que se poidan facer cargo das funcións en caso de indispoñibilidade do persoal habitual. O persoal alternativo deberá estar sometido ás mesmas garantías de seguridade que o persoal habitual.

5.3 Protección dos equipamentos [mp.eq]

5.3.1 Posto de traballo despexado [mp.eq.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	+	=

Exixirase que os postos de traballo permanezan despexados, sen máis material enriba da mesa que o requirido para a actividade que se está realizando en cada momento.

Categoría MEDIA

Este material gardarase en lugar cerrado cando non se estea utilizando.

5.3.2 Bloqueo de posto de traballo [mp.eq.2].

dimensións	A		
nivel	baixo	medio	alto
	non aplica	aplica	+

O posto de traballo bloquearase ao cabo dun tempo prudencial de inactividade, e requirirase unha nova autenticación do usuario para restablecer a actividade en curso.

Categoría ALTA

Pasado un certo tempo, superior ao anterior, cancelaranse as sesións abertas desde o citado posto de traballo.

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

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	+

Os equipamentos que abandonen as 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 incidencias de perdas ou subtraccións.

c) Establecerase un sistema de protección perimetral que minimice a visibilidade exterior e controle as opcións de acceso ao interior cando o equipamento se conecte a redes, en particular se o equipamento se conecta a redes públicas.

d) Evitarase, na medida do posible, que o equipamento conteña claves de acceso remoto á organización. Consideraranse 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 cifrado.

5.3.4 Medios alternativos [mp.eq.9]

dimensións	D		
nivel	baixo	medio	alto
	Non aplica	aplica	=

Garantirase a existencia e dispoñibilidade de medios alternativos de tratamento da información para o caso de que fallen os medios habituais. Estes medios alternativos estarán suxeitos ás mesmas garantías de protección.

Igualmente, establecerase un tempo máximo para que os equipamentos alternativos entren en funcionamento.

5.4 Protección das comunicacións [mp.com]

5.4.1 Perímetro seguro [mp.com.1].

dimensións	Todas		
categoría	básica	media	alta
	aplica	=	+

Disporase un sistema tornalumes que separe a rede interna do exterior. Todo o tráfico deberá atravesar ese tornalumes, que só deixará transitar os fluxos previamente autorizados.

Categoría ALTA

a) O sistema de tornalumes constará de dous ou máis equipamentos de diferente fabricante dispostos en forma gradual.
b) Disporanse sistemas redundantes.

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, preferentemente, produtos certificados [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 ningunha información (véxase [op.acc.5]).
b) Previranse ataques activos, garantindo que polo menos serán detectados, e activaranse os procedementos previstos de tratamento do incidente. Consideraranse ataques activos:

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

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) Valorarase positivamente o emprego de dispositivos hardware no establecemento e utilización da rede privada virtual.
b) Empregaranse, preferentemente, produtos certificados [op.pl.5].

5.4.4 Segregación de redes [mp.com.4].

dimensións	Todas		
categoría	básica	media	alta
	non aplica	non aplica	aplica

A segregación de redes acouta o acceso á información e, conseguintemente, a propagación dos incidentes de seguridade, que quedan restrinxidos ao contorno onde acontecen.
A rede dividirase en segmentos de forma que haxa:

a) Control de entrada dos usuarios que chegan a cada segmento.
b) Control de saída da información dispoñible en cada segmento.
c) As redes pódense segmentar por dispositivos físicos ou lóxicos. O punto de interconexión estará particularmente asegurado, mantido e monitorizado (como en [mp.com.1]).

5.4.5 Medios alternativos [mp.com.9].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Garantirase a existencia e dispoñibilidade de medios alternativos de comunicación para o caso de que fallen os medios habituais. Os medios alternativos de comunicación:

a) Estarán suxeitos e proporcionarán as mesmas garantías de protección que o medio habitual.
b) Garantirán un tempo máximo de entrada en funcionamento.

5.5 Protección dos soportes de información [mp.si]

5.5.1 Etiquetaxe [mp.si.1].

dimensións	C		
nivel	baixo	medio	alto
	aplica	=	=

Os soportes de información etiquetaranse de forma que, sen revelaren o seu contido, se indique o nivel de seguridade da información contida de maior cualificación.
Os usuarios deben estar capacitados para entender o significado das etiquetas, ben mediante simple inspección, ben mediante o recurso a un repositorio que o explique.

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, DVD, discos USB ou outros de natureza análoga.

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, preferentemente, produtos certificados [op.pl.5].

5.5.3 Custodia [mp.si.3].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

Aplicarase a debida dilixencia e control aos soportes de información que permanecen baixo a responsabilidade da organización, mediante as seguintes actuacións:

a) Garantindo o control de acceso con medidas físicas ([mp.if.1] e [mpl.if.7]) ou lóxicas ([mp.si.2]), ou ambas.
b) Garantindo que se respectan as exixencias de mantemento do fabricante, en especial, no referente a temperatura, humidade e outros agresores ambientais.

5.5.4 Transporte [mp.si.4].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

O responsable de sistemas garantirá que os dispositivos permanecen baixo control e que satisfán os seus requisitos de seguridade mentres están sendo desprazados dun lugar a outro.

Para iso:

a) Disporase dun rexistro de saída que identifique o transportista que recibe o soporte para o seu traslado.
b) Disporase dun rexistro de entrada que identifique o transportista que o entrega.
c) Disporase dun procedemento rutineiro que cotexe as saídas coas chegadas e levante as alarmas pertinentes cando se detecte algún incidente.
d) Utilizaranse os medios de protección criptográfica ([mp.si.2]) correspondentes ao nivel de cualificación da información contida de maior nivel.
e) Xestionaranse as claves segundo [op.exp.11].

5.5.5 Borrado e destrución [mp.si.5].

dimensións	C		
nivel	baixo	medio	alto
	no aplica	aplica	=

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

a) Os soportes que vaian ser reutilizados para outra información ou liberados a outra organización serán obxecto dun borrado seguro do seu anterior contido.
b) Destruiranse de forma segura os soportes, nos seguintes casos:

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

c) Empregaranse, preferentemente, produtos certificados [op.pl.5].

5.6 Protección das aplicacións informáticas [mp.sw].

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

dimensións	todas		
categoría	básica	media	alta
	non aplica	aplica	=

a) O desenvolvemento de aplicacións realizarase sobre un sistema diferente e separado do de produción, e non deberán 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 durante todo o ciclo de vida.
2.º Trate especificamente os datos usados en probas.
3.º Permita a inspección do código fonte.

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.

5.6.2 Aceptación e posta en servizo [mp.sw.2].

dimensións	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Antes de pasar a produción, comprobarase o correcto funcionamento da aplicación.

a) Comprobarase que:

1.º Se cumpren os criterios de aceptación en materia de seguridade.
2.º Non se deteriora a seguridade doutros compoñentes do servizo.

b) As probas realizaranse nun contorno illado (pre-produción).
c) As probas de aceptación non se realizarán con datos reais, salvo que se asegure o nivel de seguridade correspondente .

Categoría MEDIA

Realizaranse as seguintes inspeccións previas á entrada en servizo:

a) Análise de vulnerabilidades.
b) Probas de penetración.

Categoría ALTA

Realizaranse as seguintes inspeccións previas á entrada en servizo:

a) Análise de coherencia na integración nos procesos.
b) Considerarase a oportunidade de realizar unha auditoría de código fonte.

5.7 Protección da información [mp.info]

5.7.1 Datos de carácter persoal [mp.info.1].

dimensións	todas		
categoría	básica	media	alta
	aplica	aplica	aplica

Cando o sistema trate datos de carácter persoal, observarase 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.
O indicado no parágrafo anterior tamén se aplicará cando unha disposición con rango de lei se remita ás normas sobre datos de carácter persoal na protección de información.

5.7.2 Cualificación da información [mp.info.2].

dimensións	C		
nivel	baixo	medio	alto
	aplica	+	=

1. Para cualificar a información observarase o establecido legalmente sobre a súa natureza.
2. A política de seguridade establecerá quen é o responsable de cada información manexada polo sistema.
3. A política de seguridade recollerá, directa ou indirectamente, os criterios que, en cada organización, determinarán o nivel de seguridade requirido, dentro do marco establecido no artigo 43 e os criterios xerais prescritos no anexo I.
4. O responsable de cada información seguirá os criterios determinados no número anterior para asignar a cada información o nivel de seguridade requirido, e será responsable da súa documentación e aprobación formal.

5. O responsable de cada información en cada momento terá en exclusiva a potestade de modificar o nivel de seguridade requirido, de acordo cos números anteriores.

Nivel MEDIO

Redactaranse os procedementos necesarios que describan, en detalle, a forma en que se debe etiquetar e tratar a información en consideración ao nivel de seguridade que require; e precisando como se debe realizar:

a) O seu control de acceso.
b) O seu almacenamento.
c) A realización de copias.
d) A etiquetaxe de soportes.
e) A súa transmisión telemática.
f) E calquera outra actividade relacionada con tal información.

5.7.3 Cifrado da información [mp.info.3].

dimensións	C		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

Para o cifrado de información observarase o que se indica a continuación:

a) A información cun nivel alto en confidencialidade cifrarase tanto durante o seu almacenamento como durante a súa transmisión. Só estará en claro mentres se está facendo uso dela.
b) Para o uso de criptografía nas comunicacións, observarase o disposto en [mp.com.2].
c) Para o uso de criptografía nos soportes de información, observarase o disposto en [mp.si.2].

5.7.4 Sinatura electrónica [mp.info.4].

dimensións	I A		
nivel	baixo	medio	alto
	aplica	+	++

A sinatura electrónica é un mecanismo de prevención do repudio, é dicir, prevén fronte á posibilidade de que no futuro o signatario se puider desdicir da información asinada.
A sinatura electrónica garante a autenticidade do signatario e a integridade do contido.
Cando se empregue sinatura electrónica:

a) O signatario será a parte que se fai responsable da información, na medida das súas atribucións.
b) Disporase dunha política de sinatura electrónica, aprobada polo órgano superior competente que corresponda.

Nivel BAIXO

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

Nivel MEDIO

1. Os medios utilizados na sinatura electrónica serán proporcionados á cualificación da información tratada. En todo caso:

a) Empregaranse algoritmos acreditados polo Centro Criptolóxico Nacional.
b) Empregaranse, preferentemente, certificados recoñecidos.
c) Empregaranse, preferentemente, dispositivos seguros de sinatura.

2. Garantirase a verificación e 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:

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

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

b) Protexeranse a sinatura e a información mencionada na alínea anterior cun selo de tempo.
c) O organismo que solicite documentos asinados polo administrado verificará e validará a sinatura recibida no momento da recepción, anexando ou referenciando sen ambigüidade a información descrita nas alíneas a) e b).
d) A sinatura electrónica de documentos por parte da Administración anexará ou referenciará sen ambigüidade a información descrita nas alíneas a) e b).

Nivel ALTO

Aplicaranse as medidas de seguridade referentes a sinatura electrónica exixibles no nivel medio, ademais das seguintes:

a) Usaranse certificados recoñecidos.
b) Usaranse dispositivos seguros de creación de sinatura.
c) Empregaranse, preferentemente, produtos certificados [op.pl.5].

5.7.5 Selos de tempo [mp.info.5].

dimensións	T		
nivel	baixo	medio	alto
	non aplica	non aplica	aplica

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].

5.7.6 Limpeza de documentos [mp.info.6].

dimensións	C		
nivel	baixo	medio	alto
	aplica	=	=

No proceso de limpeza de documentos, retirarase destes toda a información adicional contida en campos ocultos, metadatos, comentarios ou revisións anteriores, salvo cando esa información sexa pertinente para o receptor do documento.

Esta medida é especialmente relevante cando o documento se difunde amplamente, como ocorre cando se ofrece ao público nun servidor web ou noutro tipo de repositorio de información.

Terase presente que o incumprimento desta medida pode prexudicar:

a) O mantemento da confidencialidade de información que non se debería ter revelado ao receptor do documento.

b) O mantemento da confidencialidade das fontes ou orixes da información, que non debe coñecer o receptor do documento.

c) A boa imaxe da organización que difunde o documento, por canto demostra un descoido no seu bo facer.

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

dimensións	D		
nivel	baixo	medio	alto
	non aplica	aplica	=

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

As copias de apoio desfrutarán da mesma seguridade que os datos orixinais no que se refire a integridade, confidencialidade, autenticidade e trazabilidade. En particular, considerarase a conveniencia ou necesidade de que as copias de seguridade estean cifradas para garantir a confidencialidade.

As copias de apoido deberán abarcar:

a) Información de traballo da organización.

b) Aplicacións en explotación, incluíndo os sistemas operativos.

c) Datos de configuración, servizos, aplicacións, equipamentos ou outros de natureza análoga.

d) Claves utilizadas para preservar a confidencialidade da información.

5.8 Protección dos servizos [mp.s]

5.8.1 Protección do correo electrónico [mp.s.1].

dimensións	todas		
categoría	básica	media	alta
	aplica	=	=

O correo electrónico protexerase fronte ás ameazas que lle son propias actuando do seguinte modo:

a) A información distribuída por medio de correo electrónico protexerase tanto no corpo das mensaxes coma nos anexos.

b) Protexerase a información de encamiñamento de mensaxes e establecemento de conexións.

c) Protexerase a organización fronte a problemas que se materializan por medio do correo electrónico, en concreto:

1.º Correo non solicitado, na súa expresión inglesa «spam».

2.º Programas daniños, constituídos por virus, vermes, troianos, espías ou outros de natureza análoga.

3.º Código móbil de tipo «applet».

d) Estableceranse normas de uso do correo electrónico por parte do persoal determinado. Estas normas de uso conterán:

1.º Limitacións ao uso como soporte de comunicacións privadas.

2.º Actividades de concienciación e formación relativas ao uso do correo electrónico.

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

dimensións	todas		
categoría	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 almacena no disco duro do visitante dunha páxina web a través do seu navegador, a petición do servidor da páxina, coñecido en terminoloxía inglesa como «cookies».

4.º Previranse ataques de inxección de código.

b) Previranse intentos de escalado 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 «cachés».

5.8.3 Protección fronte á denegación de servizo [mp.s.8].

dimensións	D		
nivel	baixo	medio	alto
	non aplica	aplica	+

Estableceranse medidas preventivas e reactivas fronte a ataques de denegación de servizo (DOS Denial of Service). Para iso:

a) Planificarase e dotarase o sistema de capacidade suficiente para atender a carga prevista con folgura.

b) Despregaranse tecnoloxías para previr os ataques coñecidos.

Nivel ALTO

a) Establecerase un sistema de detección de ataques de denegación de servizo.
b) Estableceranse procedementos de reacción aos ataques, incluíndo a comunicación co provedor de comunicacións.
c) Impedirase o lanzamento de ataques desde as propias instalacións prexudicando terceiros.

5.8.4 Medios alternativos [mp.s.9].

dimensiones	D		
nivel	baixo	medio	alto
	non aplica	no aplica	aplica

Garantirase a existencia e dispoñibilidade de medios alternativos para prestar os servizos no caso de que fallen os medios habituais. Estes medios alternativos estarán suxeitos ás mesmas garantías de protección que os medios habituais.

6 Desenvolvemento e complemento das medidas de seguridade.

As medidas de seguridade desenvolveranse e complementaranse segundo o establecido na disposición derradeira segunda.

7 Interpretación.

A interpretación deste anexo realizarase segundo o sentido propio das súas palabras, en relación co contexto, antecedentes históricos e lexislativos, entre os que figura o disposto nas instrucións técnicas CCN-STIC correspondentes á implementación e a diversos escenarios de aplicación tales como sedes electrónicas, servizos de validación de certificados electrónicos, servizos de datación electrónica e validación de documentos datados, atendendo o espírito e a finalidade daquelas.

ANEXO III

Auditoría da seguridade

1. *Obxecto da auditoría*

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

a) Que 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) Que existen procedementos para resolución de conflitos entre os ditos responsables.
c) Que se designaron persoas para eses roles á luz do principio de «separación de funcións».
d) Que se realizou unha análise de riscos, con revisión e aprobación anual.
e) Que se cumpren as recomendacións de protección descritas no anexo II, sobre medidas de seguridade, en función das condicións de aplicación en cada caso.
f) Que existe un sistema de xestión da seguridade da información, documentado e cun proceso regular de aprobación pola dirección.

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

a) Documentación dos procedementos.

b) Rexistro de incidencias.
c) Exame do persoal afectado: coñecemento e praxe das medidas que o afectan.

2. *Niveis de auditoría*

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

1. Auditoría a 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, indicando 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. Auditoría a sistemas de categoría MEDIA OU ALTA.

a) O informe de auditoría ditaminará sobre o grao de cumprimento deste 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 deste anexo realizarase segundo o sentido 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 á finalidade daquelas.

ANEXO IV

Glosario

Activo. Compoñente ou funcionalidade dun sistema de información susceptible de ser atacado deliberada ou accidentalmente con consecuencias para a organización. Inclúe: información, datos, servizos, aplicacións (software), equipamentos (hardware), comunicacións, recursos administrativos, recursos físicos e recursos humanos.
Análise de riscos. Utilización sistemática da información dispoñible para identificar perigos e estimar os riscos.
Auditoría da seguridade. Revisión e exame independentes dos rexistros e actividades do sistema para verificar a idoneidade dos controis do sistema, asegurar que se cumpren a política de seguridade e os procedementos operativos establecidos, detectar as infraccións da seguridade e recomendar modificacións apropiadas dos controis, da política e dos procedementos.
Autenticidade. Propiedade ou característica consistente en que unha entidade é quen di ser ou ben que garante a fonte de que proceden os datos.
Categoría dun sistema. É un nivel, dentro da escala básica-media-alta, con que se adxectiva un sistema co fin de seleccionar as medidas de seguridade necesarias para el.

A categoría do sistema recolle a visión holística do conxunto de activos como un todo harmónico, orientado á prestación duns servizos.

Confidencialidade. Propiedade ou característica consistente en que a información nin se pon á disposición nin se revela a individuos, entidades ou procesos non autorizados.

Dispoñibilidade. Propiedade ou característica dos activos consistente en que as entidades ou procesos autorizados teñen acceso a estes cando o requiren.

Incidente de seguridade. Suceso inesperado ou non desexado con consecuencias en detrimento da seguridade do sistema de información.

Integridade. Propiedade ou característica consistente en que o activo de información non foi alterado de maneira non autorizada.

Medidas de seguridade. Conxunto de disposicións encamiñadas a protexerse dos riscos posibles sobre o sistema de información, co fin de asegurar os seus obxectivos de seguridade. Pódese tratar de medidas de prevención, de disuasión, de protección, de detección e reacción, ou de recuperación.

Política de sinatura electrónica. Conxunto de normas de seguridade, de organización, técnicas e legais para determinar como se xeran, verifican e xestionan sinaturas electrónicas, incluíndo as características exixibles aos certificados de sinatura.

Política de seguridade. Conxunto de directrices plasmadas en documento escrito, que rexen a forma en que unha organización xestiona e protexe a información e os servizos que considera críticos.

Principios básicos de seguridade. Fundamentos que deben rexer toda acción orientada a asegurar a información e os servizos.

Proceso. Conxunto organizado de actividades que se levan a cabo para producir a un produto ou servizo; ten un principio e fin delimitado, implica recursos e dá lugar a un resultado.

Proceso de seguridade. Método que se segue para alcanzar os obxectivos de seguridade da organización. O proceso deséñase para identificar, medir, xestionar e manter baixo control os riscos a que se enfronta o sistema en materia de seguridade.

Trazabilidade. Propiedade ou característica consistente en que as actuacións dunha entidade poden ser imputadas exclusivamente á citada entidade.

Requisitos mínimos de seguridade. Exixencias necesarias para asegurar a información e os servizos.

Risco. Estimación do grao de exposición a que unha ameaza se materialice sobre un ou máis activos causando danos ou prexuízos á organización.

Seguridade das redes e da información. É a capacidade das redes ou dos sistemas de información de resistir, cun determinado nivel de confianza, os accidentes ou accións ilícitas ou malintencionadas que comprometan a dispoñibilidade, autenticidade, integridade e confidencialidade dos datos almacenados ou transmitidos e dos servizos que estas redes e sistemas ofrecen ou fan accesibles.

Servizos acreditados. Servizos prestados por un sistema con autorización concedida pola autoridade responsable, para tratar un tipo de información determinada, nunhas condicións precisas das dimensións de seguridade, consonte o seu concepto de operación.

Sinatura electrónica. Conxunto de datos en forma electrónica, consignados xunto a outros ou asociados con eles, que poden ser utilizados como medio de identificación do asinante.

Sistema de xestión da seguridade da información (SXSI). Sistema de xestión que, baseado no estudo dos riscos, se establece para crear, implementar, facer funcionar, supervisar, revisar, manter e mellorar a seguridade da información. O sistema de xestión inclúe a estrutura organizativa, as políticas, as actividades de planificación, as responsabilidades, as prácticas, os procedementos, os procesos e os recursos.

Sistema de información. Conxunto organizado de recursos para que a información se poida recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, pór á disposición, presentar ou transmitir.

Vulnerabilidade. Unha debilidade que pode ser aproveitada por unha ameaza.

Xestión de incidentes. Plan de acción para atender as incidencias que se dean. Ademais de resolvelas, 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.

Xestión de riscos. Actividades coordinadas para dirixir e controlar unha organización con respecto aos riscos.

Acrónimos

CCN: Centro Criptolóxico Nacional
CERT: Computer Emergency Reaction Team
INTECO: Instituto Nacional de Tecnoloxías da Comunicación
STIC: Seguridade das Tecnoloxías de Información e Comunicacións.

ANEXO V

Modelo de cláusula administrativa particular

«Cláusula administrativa particular.–En cumprimento do disposto no artigo 99.4 da Lei 30/2007, do 30 de outubro, de contratos do sector público, e o artigo 18 do Real decreto ...../....., do ….. de ..... polo que se regula o Esquema Nacional de Seguridade, o licitador incluirá referencia precisa, documentada e acreditativa de que os produtos de seguridade, equipamentos, sistemas, aplicacións ou os seus compoñentes, foron previamente certificados polo organismo de certificación do Esquema Nacional de Avaliación e Certificación de Seguridade das Tecnoloxías da Información.

No caso de que non exista a certificación indicada no parágrafo anterior, ou estea en proceso, incluirase, igualmente, referencia precisa, documentada e acreditativa de que son os máis idóneos.

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.»