REGULAMENTO DE EXECUÇÃO (UE) 2015/1502 DA COMISSÃO

de 8 de setembro de 2015

que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE ([1]), nomeadamente o artigo 8.º, n.º 3,

Considerando o seguinte:

(1) O artigo 8.º do Regulamento (UE) n.º 910/2014 prevê que os sistemas de identificação eletrónica notificados nos termos do artigo 9.º, n.º 1, especifiquem os níveis de garantia reduzido, substancial e elevado para os meios de identificação eletrónica neles produzidos.

(2) É essencial definir as especificações técnicas mínimas, as normas e os procedimentos aplicáveis, a fim de assegurar um entendimento comum dos elementos dos níveis de garantia, bem como a sua interoperabilidade, ao recensear os níveis de garantia nacionais dos sistemas de identificação eletrónica notificados relativamente aos níveis de garantia previstos no artigo 8.º, tal como previsto no artigo 12.º, n.º 4, alínea b), do Regulamento (UE) n.º 910/2014.

(3) A norma internacional ISO/IEC 29115 foi tida em consideração para as especificações e procedimentos previstos no presente ato de execução, dado que se trata da principal norma internacional existente no domínio dos níveis de segurança dos meios de identificação eletrónica. No entanto, o conteúdo do Regulamento (UE) n.º 910/2014 difere da norma internacional, em especial no que diz respeito aos requisitos de prova e verificação da identidade, bem como quanto à forma como as diferentes modalidades de identidade dos Estados-Membros e os instrumentos existentes na UE para esse efeito são tidos em consideração. Por conseguinte, embora o anexo nela se baseie, não deve fazer referência a qualquer conteúdo concreto da norma internacional ISO/IEC 29115.

(4) O presente regulamento foi concebido numa abordagem devidamente baseada nos resultados, o que também se reflete nas definições utilizadas para especificar os termos e conceitos. Estes têm em conta o objetivo do Regulamento (UE) n.º 910/2014 em relação aos níveis de segurança dos meios de identificação eletrónica. Por conseguinte, o projeto-piloto de grande escala STORK, incluindo as especificações aí desenvolvidas, bem como as definições e conceitos da norma ISO/IEC 29115, devem ser tidos na máxima conta ao estabelecer as especificações e procedimentos previstos no presente ato de execução.

(5) Em função do contexto em que um elemento de prova de identidade tem de ser verificado, as fontes qualificadas podem assumir muitas formas, nomeadamente registos, documentos ou organismos. As fontes qualificadas que podem ser diferentes nos diversos Estados-Membros, mesmo num contexto semelhante.

(6) Os requisitos de prova e verificação da identidade devem ter em conta os diferentes sistemas e práticas, assegurando simultaneamente um grau de garantia suficientemente elevado para estabelecer a confiança necessária. Portanto, a aceitação dos procedimentos utilizados anteriormente para outros fins que não a produção de meios de identificação eletrónica deve estar subordinada à confirmação de que esses procedimentos cumprem os requisitos previstos para o nível de garantia correspondente.

([1]) JO L 257 de 28.8.2014, p. 73.

(7) Em geral são utilizados certos fatores de autenticação, como a partilha de segredos comerciais, dispositivos físicos e atributos físicos. No entanto, a utilização de um maior número de fatores de autenticação, em especial de diferentes categorias, deve ser incentivada para aumentar a segurança do processo de autenticação.

(8) O presente regulamento não deve afetar os direitos de representação das pessoas coletivas. No entanto, o anexo deve prever os requisitos para a ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas.

(9) A importância da segurança da informação e dos sistemas de gestão de serviços deve ser reconhecida, tal como deve ser reconhecida a importância do emprego de metodologias reconhecidas e da aplicação dos princípios consagrados em normas como a ISO/IEC 27000 e a série de normas ISO/IEC 20000.

(10) As boas práticas relativamente aos níveis de garantia nos Estados-Membros também devem ser tidas em conta.

(11) A certificação de segurança informática baseada em normas internacionais é um instrumento importante para verificar a conformidade dos produtos com os requisitos previstos no presente ato de execução.

(12) O Comité referido no artigo 48.º do Regulamento (UE) n.º 910/2014 não emitiu um parecer no prazo estipulado pela respetiva presidência,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

1. Os níveis de garantia reduzido, substancial e elevado dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado são determinados com base nas especificações e procedimentos definidos no anexo.

2. As especificações e procedimentos definidos no anexo devem ser utilizados para especificar o nível de garantia dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado, para determinar a confiança e qualidade dos seguintes elementos:

a) A inscrição, conforme definida no ponto 2.1 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alínea a), do Regulamento (UE) n.º 910/2014;

b) A gestão dos meios de identificação eletrónica, conforme definida no ponto 2.2 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alíneas b) e f), do Regulamento (UE) n.º 910/2014;

c) A autenticação, conforme definida no ponto 2.3 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alínea c), do Regulamento (UE) n.º 910/2014;

d) A gestão e organização, conforme definidas no ponto 2.4 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alíneas d) e e), do Regulamento (UE) n.º 910/2014.

3. Quando os meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado cumprirem os requisitos do nível de garantia mais elevado, presume-se que cumprem os requisitos equivalentes de um nível de garantia inferior.

4. Salvo indicação em contrário na parte relevante do anexo, todos os elementos enumerados no anexo para um determinado nível de garantia do meio de identificação eletrónica produzido no âmbito de um sistema de identificação eletrónica notificado devem ser cumpridos para se atingir o nível de garantia em questão.

Artigo 2.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 8 de setembro de 2015.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

ANEXO

Especificações técnicas e procedimentos para a atribuição dos níveis de garantia reduzido, substancial e elevado dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado

1. Definições aplicáveis

Para efeitos do presente anexo, entende-se por:

1) «Fonte qualificada», qualquer fonte, independentemente da sua forma, que pode ser considerada fiável para fornecer dados exatos, informações e/ou elementos de prova que podem ser utilizados para comprovar a identidade;

2) «Fator de autenticação», um elemento confirmado como ligado a uma pessoa, que se enquadra numa das seguintes categorias:

   a) «Fator de autenticação baseado na posse», um fator de autenticação em que a pessoa em causa tem de provar a sua posse;

   b) «Fator de autenticação baseado no conhecimento», um fator de autenticação em que a pessoa em causa tem de demonstrar o conhecimento do mesmo;

   c) «Fator de autenticação inerente», um fator de autenticação que tem por base um atributo físico de uma pessoa singular, que a pessoa em causa tem de demonstrar possuir;

3) «Autenticação dinâmica», um processo eletrónico que utiliza criptografia ou outras técnicas para fornecer um meio de criar a pedido uma prova eletrónica de que a pessoa em causa controla ou tem na sua posse os dados de identificação e que se altera com cada autenticação entre a pessoa em causa e o sistema que verifica a sua identidade;

4) «Sistema de gestão da segurança das informações», um conjunto de processos e procedimentos destinados a garantir níveis aceitáveis de riscos associados à segurança da informação.

2. Especificações técnicas e procedimentos

Os elementos das especificações técnicas e procedimentos descritos no presente anexo devem ser utilizados para determinar a forma como os requisitos e critérios estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 devem ser aplicados aos meios de identificação eletrónica produzidos por um sistema de identificação eletrónica.

2.1. *Inscrição*

2.1.1. Pedido e registo

Nível de garantia	Elementos necessários
Reduzido	1. Assegurar que o requerente tem conhecimento dos termos e condições relacionados com a utilização dos meios de identificação eletrónica. 2. Assegurar que o requerente tem conhecimento das precauções recomendadas relativamente à utilização dos meios de identificação eletrónica. 3. Recolher os dados de identificação necessários para a prova e verificação da identidade.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.1.2. Prova e verificação da identidade (pessoa singular)

Nível de garantia	Elementos necessários
Reduzido	1. Pode considerar-se que a pessoa está na posse de elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica e que representam a identidade declarada. 2. Pode considerar-se que os elementos de prova são genuínos, ou que são conformes com uma fonte qualificada e parecem ser válidos. 3. Sabe-se, de acordo com uma fonte qualificada, que a identidade declarada existe e pode presumir-se que a pessoa que declara a identidade é a própria.
Substancial	Idênticos ao nível reduzido, acrescidos de uma das alternativas enumeradas nos pontos 1 a 4: 1. Verificou-se que a pessoa está na posse de elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica e que representam a identidade declarada e Os elementos de prova são controlados para verificar se são genuínos; ou, de acordo com uma fonte qualificada, sabe-se que existem e que se referem a uma pessoa real e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de elementos de prova perdidos, roubados, suspensos, revogados ou caducados; ou 2. Um documento de identidade é apresentado durante um processo de registo no Estado-Membro em que o documento foi emitido e o documento parece dizer respeito à pessoa que o apresenta e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de documentos perdidos, roubados, suspensos, revogados ou caducados; ou 3. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.2 para o nível garantia substancial, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho ([1]), ou por um organismo equivalente; ou 4. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia substancial ou elevado, e tendo em conta o risco de uma alteração dos dados de identificação pessoal, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia substancial ou elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente.

Nível de garantia	Elementos necessários
Elevado	Têm de ser respeitados os requisitos do ponto 1 ou 2: 1. Idênticos ao nível substancial, acrescidos de uma das alternativas enumeradas nos pontos a) a c): a) Nos casos em que se verifique que a pessoa está na posse de elementos de identificação com fotografia ou dados biométricos reconhecidos pelo Estado-Membro em que se efetua o pedido de identidade eletrónica, e que os elementos de prova representem a identidade declarada, os elementos de prova são controlados para verificar se esta é válida de acordo com uma fonte qualificada; e O requerente é identificado com a identidade declarada através da comparação de uma ou mais características físicas da pessoa com uma fonte qualificada; ou b) Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.2 para o nível garantia elevado, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, ou por um organismo equivalente; e Foram tomadas medidas para demonstrar que os resultados dos procedimentos anteriores continuam a ser válidos; ou c) Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia elevado, e tendo em conta o risco de uma alteração dos dados de identificação pessoal, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente. e Foram tomadas medidas para demonstrar que os resultados do anterior procedimento de emissão de um meio de identificação eletrónica notificado continuam válidos. OU 2. Se o requerente não apresentar quaisquer elementos de identificação reconhecidos com fotografia ou dados biométricos, são aplicados os mesmos procedimentos utilizados a nível nacional no Estado-Membro da entidade responsável pelo registo para obter tais elementos de identificação reconhecidos com fotografia ou dados biométricos.

(1) Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

2.1.3. Prova e verificação da identidade (pessoa coletiva)

Nível de garantia	Elementos necessários
Reduzido	1. A identidade declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica.

Nível de garantia	Elementos necessários
	2. Os elementos de prova aparentam ser válidos e genuínos, ou presume-se a sua existência de acordo com uma fonte qualificada, quando a inclusão de uma pessoa coletiva na fonte autorizada é voluntária e está regulamentada por um acordo entre a pessoa coletiva e a fonte qualificada. 3. A pessoa coletiva não é reconhecida por uma fonte qualificada com um estatuto que a impeça de atuar como pessoa coletiva.
Substancial	Idênticos ao nível reduzido, acrescidos de uma das alternativas enumeradas nos pontos 1 a 3: 1. A identidade da pessoa coletiva declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica, incluindo a designação da pessoa coletiva, a forma jurídica e (quando aplicável) o número de registo. e Os elementos de prova são analisados a fim de determinar a sua autenticidade, ou se a sua existência é conhecida em conformidade com uma fonte qualificada, quando a inclusão da pessoa coletiva na fonte qualificada é uma condição para a pessoa coletiva exercer a atividade no seu setor e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa coletiva não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de documentos perdidos, roubados, suspensos, revogados ou caducados; ou 2. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.3 para o nível garantia substancial, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 ou por um organismo equivalente; ou 3. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia substancial ou elevado, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia substancial ou elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente.
Elevado	Idênticos ao nível substancial, acrescidos de uma das alternativas enumeradas nos pontos 1 a 3: 1. A identidade da pessoa coletiva declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica, incluindo a designação da pessoa coletiva, a forma jurídica e, pelo menos, um identificador único que represente a pessoa coletiva, utilizado num contexto nacional. e Os elementos de prova são controlados para verificar a sua validade de acordo com uma fonte qualificada; ou

Nível de garantia	Elementos necessários
	2. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.3 para o nível garantia elevado, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 ou por um organismo equivalente; e Foram tomadas medidas para demonstrar que os resultados dos procedimentos anteriores continuam a ser válidos; ou 3. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia elevado, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente. e Foram tomadas medidas para demonstrar que os resultados do anterior procedimento de emissão de um meio de identificação eletrónica notificado continuam válidos.

2.1.4. Ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas

Se for caso disso, são aplicáveis as seguintes condições à ligação entre o meios de identificação eletrónica de uma pessoa singular e os meios de identificação eletrónica de uma pessoa coletiva («ligação»):

1) É possível suspender e/ou revogar uma ligação. O ciclo de vida de uma ligação (por exemplo, ativação, suspensão, renovação, revogação) é gerido de acordo com os procedimentos reconhecidos a nível nacional.

2) A pessoa singular cujos meios de identificação eletrónica estão ligados aos meios de identificação eletrónica da pessoa coletiva pode delegar o exercício da ligação noutra pessoa singular com base em procedimentos reconhecidos a nível nacional. No entanto, a pessoa singular que efetua a delegação permanecerá responsável.

3) A ligação efetua-se do seguinte modo:

Nível de garantia	Elementos necessários
Reduzido	1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia reduzido ou superior. 2. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional. 3. A pessoa singular não é reconhecida por uma fonte qualificada com um estatuto que a impeça de agir em nome da pessoa coletiva.
Substancial	Ponto 3 do nível reduzido, acrescido de: 1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia substancial ou elevado.

Nível de garantia	Elementos necessários
	2. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional, o que resultou na inscrição da ligação numa fonte qualificada. 3. A ligação foi verificada com base nas informações provenientes de uma fonte qualificada.
Elevado	Ponto 3 do nível reduzido e ponto 2 do nível substancial, acrescido de: 1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia elevado. 2. A ligação foi verificada com base num identificador único que representa a pessoa coletiva, utilizado no contexto nacional; e, com base nas informações de uma fonte qualificada que representam de modo único uma pessoa singular.

2.2. *Gestão dos meios de identificação eletrónica*

2.2.1. Características e configuração dos meios de identificação eletrónica

Nível de garantia	Elementos necessários
Reduzido	1. Os meios de identificação eletrónica utilizam, pelo menos, um fator de autenticação. 2. Os meios de identificação eletrónica são concebidos de modo a assegurar que o emitente toma as medidas razoáveis para verificar que só são utilizados sob o controlo ou na posse da pessoa a que pertencem.
Substancial	1. Os meios de identificação eletrónica utilizam, pelo menos, dois fatores de autenticação de diferentes categorias. 2. Os meios de identificação eletrónica são concebidos de modo a permitir presumir que só são utilizados sob o controlo ou na posse da pessoa a que pertencem.
Elevado	Nível substancial, acrescido de: 1. O meio de identificação eletrónica protege contra a duplicação e a manipulação, bem como contra ataques de elevado potencial 2. O meio de identificação eletrónica é concebido de forma a poder ser eficazmente protegido pela pessoa a que pertence contra a utilização por terceiros.

2.2.2. Emissão, entrega e ativação

Nível de garantia	Elementos necessários
Reduzido	Após a emissão, os meios de identificação eletrónica são entregues através de um mecanismo que permite presumir que só chegam à pessoa a que se destinam.
Substancial	Após a emissão, os meios de identificação eletrónica são entregues através de um mecanismo que permite presumir que só ficam na posse da pessoa a que pertencem.
Elevado	O processo de ativação verifica se os meios de identificação eletrónica foram entregues e ficaram na posse da pessoa a que pertencem.

2.2.3. Suspensão, revogação e reativação

Nível de garantia	Elementos necessários
Reduzido	1. É possível suspender e/ou revogar um meio de identificação eletrónica de uma forma atempada e eficaz. 2. Foram tomadas medidas para impedir a sua revogação, suspensão e/ou reativação não autorizadas. 3. A reativação só terá lugar se os mesmos requisitos de garantia estabelecidos antes da suspensão ou revogação continuarem a verificar-se.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.2.4. Renovação e substituição

Nível de garantia	Elementos necessários
Reduzido	Tendo em conta o risco de alteração dos dados de identificação pessoal, a renovação ou substituição devem cumprir os mesmos requisitos de garantia do processo inicial de prova e verificação da identidade, ou basear-se num meio de identificação eletrónica válido do mesmo nível de garantia ou superior.
Substancial	Idênticos ao nível reduzido.
Elevado	Nível reduzido, acrescido de: Em caso de renovação ou substituição com base num meio de identificação eletrónica válido, os dados de identificação são verificados junto de uma fonte qualificada.

2.3. *Autenticação*

Esta secção debruça-se sobre os perigos associados à utilização do mecanismo de autenticação e enumera os requisitos para cada nível de garantia. As verificações previstas nesta secção devem ser entendidas como proporcionais aos riscos de determinado nível de garantia.

2.3.1. Mecanismo de autenticação

O quadro seguinte apresenta os requisitos por nível de garantia relativos ao mecanismo de autenticação, através do qual a pessoa singular ou coletiva utiliza o meio de identificação eletrónica para confirmar a sua identidade perante um utilizador.

Nível de garantia	Elementos necessários
Reduzido	1. A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação eletrónica e da sua validade. 2. Nos casos em que os dados de identificação pessoal são armazenados no quadro do mecanismo de autenticação, essas informações devem ser securizadas de modo a assegurar a sua proteção contra as perdas e fuga, incluindo a análise fora de linha. 3. O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque básica-reforçada possa subverter os mecanismos de autenticação.

Nível de garantia	Elementos necessários
Substancial	Nível reduzido, acrescido de: 1. A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação eletrónica e da sua validade através de uma autenticação dinâmica. 2. O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque moderada possa subverter os mecanismos de autenticação.
Elevado	Nível substancial, acrescido de: O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque elevada possa subverter os mecanismos de autenticação.

2.4. *Gestão e organização*

Todos os participantes que prestam um serviço relacionado com a identificação eletrónica num contexto transfronteiriço (a seguir designados «prestadores») devem dispor de práticas documentadas de gestão da segurança da informação, políticas e abordagens em matéria de gestão do risco e outros controlos reconhecidos que ofereçam garantias aos órgãos de gestão responsáveis pelos sistemas de identificação eletrónica dos respetivos Estados-Membros de que estão em vigor práticas eficazes. Ao longo de toda a secção 2.4, todos os requisitos/ /elementos devem ser entendidos como proporcionais aos riscos de determinado nível.

2.4.1. Disposições gerais

Nível de garantia	Elementos necessários
Reduzido	1. Os prestadores de serviços operacionais abrangidos pelo presente regulamento são uma autoridade pública ou uma entidade jurídica reconhecida como tal pelo direito nacional de um Estado-Membro, com uma organização estabelecida e plenamente operacional em todas as partes relevantes para a prestação dos serviços. 2. Os prestadores têm de cumprir todos os requisitos legais que lhes incumbem no âmbito da operação e prestação dos serviços, incluindo os tipos de informações que podem ser solicitadas, a forma como a verificação da identidade é realizada, o tipo de informações que podem ser conservadas e durante quanto tempo. 3. Os prestadores devem poder demonstrar a sua capacidade para assumirem os riscos decorrentes da responsabilidade por danos, bem como dispor dos recursos financeiros suficientes para garantir a continuidade das operações e da prestação dos serviços. 4. Os prestadores são responsáveis pelo cumprimento de qualquer dos compromissos subcontratados a outra entidade e pela conformidade com o regime, como se eles próprios prestassem os serviços. 5. Os sistemas de identificação eletrónica não instituídos pela legislação nacional devem prever um plano de cessação efetiva. Esse plano deve prever interrupções ordenadas do serviço ou a continuação por outro prestador, a forma como as autoridades competentes e os utilizadores finais são informados, bem como os pormenores sobre a forma como os registos devem ser protegidos, mantidos e destruídos em conformidade com a política do sistema.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.2. Publicação de notificações e informações para os utilizadores

Nível de garantia	Elementos necessários
Reduzido	1. Existe uma definição de serviços publicada que inclui todos os termos, condições e taxas, incluindo eventuais restrições à sua utilização. A definição de serviços deve incluir uma política de proteção da privacidade. 2. Devem ser postos em prática políticas e procedimentos adequados para assegurar que os utilizadores do serviço são informados atempadamente e de forma fiável de quaisquer alterações da definição ou das condições de quaisquer serviços ou da política de proteção da privacidade dos serviços em causa. 3. Devem ser postas em vigor políticas e procedimentos adequados para que os pedidos de informações recebam respostas exaustivas e exatas.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.3. Gestão da segurança da informação

Nível de garantia	Elementos necessários
Reduzido	Existe um sistema de gestão da segurança da informação eficaz para a gestão e controlo dos riscos da segurança da informação.
Substancial	Nível reduzido, acrescido de: O sistema de gestão da segurança das informações respeita normas ou princípios comprovados de gestão e controlo dos riscos de segurança da informação.
Elevado	Idênticos ao nível substancial.

2.4.4. Manutenção de registos

Nível de garantia	Elementos necessários
Reduzido	1. Registar e conservar as informações relevantes utilizando um sistema de gestão de arquivos eficaz, tendo em conta a legislação aplicável e as boas práticas em matéria de proteção e conservação de dados. 2. Manter, na medida em que tal seja permitido pela legislação nacional ou outras disposições administrativas nacionais, e proteger os registos enquanto forem necessários para fins de auditoria e investigação de violações da segurança, e de manutenção, após o que os registos devem ser destruídos de forma segura.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.5. Instalações e pessoal

O quadro seguinte apresenta os requisitos relativos a instalações e pessoal e, quando aplicável, a subcontratantes que desempenham funções abrangidas pelo presente regulamento. A conformidade com todos os requisitos deve ser proporcional ao nível de risco associado ao nível de garantia em questão.

Nível de garantia	Elementos necessários
Reduzido	1. Existem procedimentos que asseguram que o pessoal e os subcontratantes são devidamente formados, qualificados e experientes nas competências necessárias para executar as funções que desempenham. 2. Existe pessoal e subcontratantes em número suficiente para prestar de forma adequada os serviços com os recursos conformes com as suas políticas e procedimentos. 3. As instalações utilizadas para prestar o serviço são permanentemente monitorizadas para detetar e proteger contra os danos causados por fenómenos ambientais, o acesso não autorizado e outros fatores que possam afetar a segurança do serviço. 4. As instalações utilizadas para prestar o serviço garantem que o acesso às zonas de conservação ou tratamento de informações pessoais, criptográficas ou outras informações sensíveis é limitado ao pessoal ou aos subcontratantes autorizados
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.6. Controlos técnicos

Nível de garantia	Elementos necessários
Reduzido	1. Existem controlos técnicos proporcionados para gerir os riscos que se colocam à segurança dos serviços e proteger a confidencialidade, a integridade e a disponibilidade das informações tratadas. 2. Os canais de comunicação eletrónicos utilizados para intercâmbio de informações sensíveis ou pessoais estão protegidos contra a interceção, a manipulação e a reprodução. 3. O acesso a material criptográfico sensível, se utilizado para a emissão de meios de identificação eletrónica e para a autenticação, está estritamente limitado às funções e aplicações que exijam esse acesso. Deve garantir-se que este material nunca é armazenado de forma persistente em forma de texto. 4. Existem procedimentos para garantir que a segurança se mantém ao longo do tempo e tem capacidade de resposta às alterações dos níveis de risco, aos incidentes e às falhas de segurança. 5. Todos os suportes que contenham dados criptográficas ou pessoais ou outros dados sensíveis, são armazenados, transportados e eliminados de forma segura.
Substancial	Idênticos ao nível reduzido, acrescido de: O material criptográfico sensível, se utilizado para a emissão de meios de identificação eletrónica e a autenticação, é protegido contra a manipulação abusiva
Elevado	Idênticos ao nível substancial.

2.4.7. Conformidade e auditoria

Nível de garantia	Elementos necessários
Reduzido	São realizadas auditorias internas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes.

Nível de garantia	Elementos necessários
Substancial	São realizadas auditorias independentes internas ou externas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes.
Elevado	1. São realizadas auditorias independentes externas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes. 2. Quando o regime é gerido diretamente por um organismo governamental, é objeto de uma auditoria realizada de acordo com o direito nacional.