第 300/2018 號行政長官批示

行政長官行使《澳門特別行政區基本法》第五十條賦予的職權，並根據第35/2018號行政法規《電子服務》第十六條的規定，作出本批示。

一、核准附於本批示並為其組成部分的《使用者帳戶系統保障水平的技術規格規章》。

二、本批示自二零一九年一月一日起生效。

二零一八年十二月十九日

行政長官　崔世安

使用者帳戶系統保障水平的技術規格規章

第一章
一般規定

第一條
標的

一、本規章訂定在使用者帳戶系統範圍內，適用於以電子方式組織及容許對使用者身份作核實的各項程序的技術規格。

二、上款所指的技術規格包括以下事宜：

（一）指出使用者帳戶系統的各個要素類別；

（二）指出各個要素類別的保障水平及電子身份識別工具；

（三）訂定在各個要素類別中須執行的程序；

（四）在每一程序中達至各個保障水平的標準及指標。

第二條
定義

為適用本規章的規定，下列用語的含義為：

（一）“使用者帳戶系統”：是指用於管理設立電子身份、生成電子身份識別工具及以電子方式執行核實使用者身份程序所需的工具的一系列規則、方法及程序；

（二）“電子身份識別工具”：是指持有人在數字化接待時使用的尤其是登入密碼、一次性密碼、安全驗證碼、生物識別數據、

Despacho do Chefe do Executivo n.º 300/2018

Usando da faculdade conferida pelo artigo 50.º da Lei Básica da Região Administrativa Especial de Macau e nos termos do artigo 16.º do Regulamento Administrativo n.º 35/2018 (Serviços electrónicos), o Chefe do Executivo manda:

1. É aprovado o regulamento sobre especificações técnicas relativas aos níveis de garantia dos sistemas de contas de utilizador, anexo ao presente despacho e do qual faz parte integrante.

2. O presente despacho entra em vigor no dia 1 de Janeiro de 2019.

19 de Dezembro de 2018.

O Chefe do Executivo, *Chui Sai On*.

Regulamento sobre especificações técnicas relativas aos níveis de garantia dos sistemas de contas de utilizador

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objecto

1. O presente regulamento estabelece as especificações técnicas aplicáveis, no âmbito de um sistema de conta de utilizador, aos diversos procedimentos que organizam e permitem a verificação, por meios electrónicos, da identidade do utilizador.

2. As especificações técnicas referidas no número anterior abrangem os seguintes assuntos:

1) Indicação dos grupos de elementos de um sistema de conta de utilizador;

2) Indicação dos níveis de garantia dos grupos de elementos e dos meios de identificação electrónica;

3) Definição dos processos a executar em cada grupo de elementos;

4) Critérios e directrizes para alcançar os níveis de garantia em cada processo.

Artigo 2.º
Definições

Para efeitos do presente regulamento, entende-se por:

1) «Sistema de conta de utilizador», o conjunto de regras, métodos e procedimentos para a gestão dos instrumentos necessários à criação de identidades electrónicas, à produção de meios de identificação electrónica e à execução, por meios electrónicos, do processo de verificação de identidade do utilizador;

2) «Meio de identificação electrónica», uma combinação de dados, nomeadamente senha de acesso, senha de uso único, código seguro de verificação, dados biométricos, certificado electrónico,

電子證書、高級電子簽名或合格電子簽名等數據組合，以標識其身份及登入者和在數字化接待過程中作出行為的人的身份；

（三）“認證”：是指在核實使用者身份程序中所執行的工作，以讓利害關係人證明其為正當使用者；

（四）“認證因素”：是指確認已與正當使用者連接的一個要素，其可以是持有類別因素、知識類別因素或屬性類別因素；

（五）“持有類別認證因素”：是指以正當使用者管控的一種要素作為認證因素，尤指身份證明文件（居民身份證、護照）、載有憑證或私鑰的實體設備；

（六）“知識類別認證因素”：是指以正當使用者所知的一種要素作為認證因素，尤指登入密碼、一次性密碼、個人識別號碼（PIN）；

（七）“屬性類別認證因素”：是指以正當使用者的身體特性作為認證因素，尤指其生物識別特徵資料；

（八）“動態認證”：是指一個利用密碼或其他技術，按要求提供一種電子證明產生工具的電子程序，該電子證明表示某人或實體管控或持有相關身份識別數據，而身份核實系統在每次認證人或實體時所產生的電子證明均不同；

（九）“合格來源”：是指一個能可靠地提供用以確認利害關係人身份的準確數據、資訊或證明資料的澳門特別行政區內外、形式不論的紀錄、部門或實體。

第三條

使用者帳戶系統

一、透過互聯網提供數字化接待的公共部門和實體採用使用者帳戶系統，以便可以核實每個使用者的身份，以及核實數字化接待中執行某些操作所需的准許。

二、除了負責管理及組織使用者帳戶系統的公共部門或公共實體外，其他實體亦可參與該使用者帳戶系統，尤其是參與執行與使用者帳戶扣聯的電子身份識別工具的生成、啟動及管理程序。

三、負責管理及組織某一使用者帳戶系統的公共部門或公共實體，應透過適當方式，尤其在本身的互聯網網站內公佈參與該使用者帳戶系統的實體名單。

四、使用者帳戶系統可要求源自合格來源的資訊或證明資料。

assinatura electrónica avançada ou assinatura electrónica qualificada que o respectivo titular utiliza, no atendimento digital, para demonstrar a sua identidade e autoria do acesso e dos actos praticados no atendimento digital;

3) «Autenticação», a acção executada num processo de verificação de identidade do utilizador, para o interessado em causa demonstrar que é o utilizador legítimo;

4) «Factor de autenticação», um elemento que está confirmado como ligado ao utilizador legítimo, o qual pode ser baseado na posse, no conhecimento ou intrínseco;

5) «Factor de autenticação baseado na posse», um factor de autenticação que é um elemento que está sob controlo do utilizador legítimo, nomeadamente documento de identificação (BIR, passaporte), dispositivo físico que contém uma credencial ou chave privada;

6) «Factor de autenticação baseado no conhecimento», um factor de autenticação que é um elemento que o utilizador legítimo conhece, nomeadamente senha de acesso, senha de uso único, número de identificação pessoal (PIN);

7) «Factor de autenticação intrínseco», um factor de autenticação que tem por base um atributo físico do utilizador legítimo, nomeadamente informação das suas características biométricas;

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

9) «Fonte qualificada», um registo, um serviço ou uma entidade, na Região Administrativa Especial de Macau, doravante designada por RAEM, ou no exterior, independentemente da sua forma, que é considerada fiável para fornecer dados exactos, informações ou elementos de prova que podem ser utilizados para confirmar a identidade do interessado.

Artigo 3.º

Sistema de conta de utilizador

1. Os serviços e entidades públicos que disponibilizam, através da *Internet*, atendimento digital usam um sistema de conta de utilizador para poderem verificar a identidade de cada utilizador e a respectiva permissão para executar determinadas operações no atendimento digital.

2. Podem participar num sistema de conta de utilizador, além do serviço público ou entidade pública responsável pela sua gestão e organização, outras entidades, nomeadamente na execução dos processos de produção, activação e gestão dos meios de identificação electrónica vinculados a uma conta de utilizador.

3. O serviço público ou entidade pública responsável pela gestão e organização de um sistema de conta de utilizador publicita pela forma adequada, nomeadamente no respectivo sítio na *Internet*, a lista das entidades que participem nesse mesmo sistema de conta de utilizador.

4. Podem ser solicitadas informações ou elementos de prova provenientes de fonte qualificada.

第四條

使用者帳戶的種類

一、使用者帳戶系統內具有自然人使用者帳戶和實體使用者帳戶。

二、下列者可成為實體使用者帳戶持有人：

（一）澳門特別行政區政府架構內的行政機關、部門或實體；

（二）上項未包括的公法實體；

（三）法人；

（四）自然人商業企業主；

（五）無法律人格的組織，尤其澳門特別行政區內的樓宇管理機關。

三、上款（一）及（二）項規定的行政機關、部門或實體，如其用於自動化活動的資訊設備使用本身的電子身份識別工具，應在使用者帳戶系統內登記該等設備。

四、上款規定的登記尤其透過下列任一技術上較為適當的方式進行：

（一）將資訊設備所用的電子身份識別工具與資訊設備所屬的行政機關、部門或實體的使用者帳戶扣聯；

（二）為資訊設備開立實體使用者帳戶，該帳戶從開立起即與資訊設備所屬的行政機關、部門或實體的使用者帳戶連接。

第五條

保障水平

一、保障水平表示使用者帳戶系統及相關電子身份識別工具的各個要素類別的可靠度。

二、滿意級保障水平對所聲明的身份給予有限的可靠度，表示已遵守規則及技術程序，尤其在技術控制方面，目的是降低不適當使用或更改身份的風險。

三、高級保障水平對所聲明的身份給予高度的可靠度，表示已遵守規則及技術程序，尤其在技術控制方面，目的是大幅度降低不適當使用或更改身份的風險。

四、非常高級保障水平對所聲明的身份給予非常高的可靠度，表示已遵守規則及技術程序，尤其在技術控制方面，目的是避免不適當使用或更改身份。

Artigo 4.º

Tipos de conta de utilizador

1. No sistema de conta de utilizador há contas de utilizador de pessoa singular e contas de utilizador de entidade.

2. Pode ser titular de conta de utilizador de entidade:

1) Órgão administrativo, serviço ou entidade que integre a estrutura do Governo da RAEM;

2) Entidade de Direito Público não abrangida na alínea anterior;

3) Pessoa colectiva;

4) Empresário comercial pessoa singular;

5) Organização sem personalidade jurídica, nomeadamente órgão de condomínio de prédio situado na RAEM.

3. O órgão administrativo, serviço ou entidade previsto nas alíneas 1) e 2) do número anterior deve inscrever no sistema de conta de utilizador os respectivos equipamentos informáticos que se destinem a actuação automatizada, quando tais equipamentos apliquem meios de identificação electrónica próprios.

4. A inscrição prevista no número anterior é concretizada pela forma tecnicamente mais adequada, nomeadamente por uma das seguintes modalidades:

1) Os meios de identificação electrónica aplicados pelo equipamento informático ficam vinculados à conta de utilizador do órgão administrativo, serviço ou entidade a quem pertence esse equipamento;

2) Abertura de conta de utilizador de entidade para o equipamento informático, a qual fica ligada, desde a abertura, à conta de utilizador do órgão administrativo, serviço ou entidade a quem pertence esse equipamento.

Artigo 5.º

Níveis de garantia

1. Os níveis de garantia indicam o grau de confiança dos grupos de elementos de um sistema de conta de utilizador e dos respectivos meios de identificação electrónica.

2. O nível de garantia satisfatório confere um nível de confiança limitado relativamente à identidade declarada e corresponde à observância de regras e procedimentos técnicos, nomeadamente controlos técnicos, cuja finalidade é reduzir o risco de utilização ou alteração indevida da identidade.

3. O nível de garantia elevado confere um nível de confiança amplo relativamente à identidade declarada e corresponde à observância de regras e procedimentos técnicos, nomeadamente controlos técnicos, cuja finalidade é reduzir substancialmente o risco de utilização ou alteração indevida da identidade.

4. O nível de garantia muito elevado confere um nível de confiança muito amplo relativamente à identidade declarada e corresponde à observância de regras e procedimentos técnicos, nomeadamente controlos técnicos, cuja finalidade é evitar a utilização ou a alteração indevida da identidade.

第六條

使用者帳戶系統的要素類別

一、必須符合使用者帳戶系統下列各要素類別對某一保障水平所定的要素，方為達至該保障水平：

（一）開立使用者帳戶階段的要素類別；

（二）電子身份識別工具管理階段的要素類別；

（三）認證階段的要素類別；

（四）系統管理及組織的要素類別。

二、為達至某一保障水平，必須符合為該水平設定的所有要素，但有相反規定者除外。

Artigo 6.º

Grupos de elementos do sistema de conta de utilizador

1. O nível de garantia é alcançado em resultado do cumprimento dos elementos enumerados para esse mesmo nível de garantia nos seguintes grupos de elementos do sistema de conta de utilizador:

1) Grupo de elementos da fase de abertura de conta de utilizador;

2) Grupo de elementos da fase de gestão dos meios de identificação electrónica;

3) Grupo de elementos da fase de autenticação;

4) Grupo de elementos de gestão e organização do sistema.

2. Salvo disposição em contrário, todos os elementos enumerados para um determinado nível de garantia devem ser cumpridos para se atingir esse nível de garantia.

第二章
開立使用者帳戶階段

CAPÍTULO II
Fase de abertura de conta de utilizador

第七條

開立使用者帳戶階段的範圍

一、開立使用者帳戶階段包括開立申請、確認身份、電子身份識別工具之間的連接及內部記錄的程序；

二、上款規定的各個程序可全部由使用者帳戶系統的責任實體執行，或由參與生成使用者帳戶系統電子身份識別工具的多個實體協同執行。

Artigo 7.º

Âmbito da fase de abertura de conta de utilizador

1. A fase de abertura de conta de utilizador inclui os processos de pedido de abertura, confirmação da identidade, ligação entre meios de identificação electrónica e registo interno.

2. Os processos previstos no número anterior podem ser todos executados, na íntegra, pela entidade responsável pelo sistema de conta de utilizador ou ser executados de forma integrada por várias entidades que participem na produção dos meios de identificação electrónica desse sistema de conta de utilizador.

第八條

開立申請的程序

一、在使用者帳戶的開立申請程序中，應符合下列要素：

（一）確保利害關係人或其法定代表知悉電子身份識別工具的使用條款；

（二）確保利害關係人或其法定代表知悉使用電子身份識別工具的建議預防措施；

（三）收集開立帳戶所需的身份識別資料。

二、上款的規定適用於所有保障水平。

Artigo 8.º

Processo de pedido de abertura

1. No processo do pedido de abertura de conta de utilizador devem ser cumpridos os seguintes elementos:

1) Assegurar que o interessado ou o seu representante legal tem conhecimento dos termos e condições relacionados com a utilização dos meios de identificação electrónica;

2) Assegurar que o interessado ou o seu representante legal tem conhecimento das precauções recomendadas relativamente à utilização dos meios de identificação electrónica;

3) Recolher a informação de identificação que é necessária para a abertura de conta.

2. O disposto no número anterior é aplicável a todos os níveis de garantia.

第九條

提交開立申請

一、自然人使用者帳戶的開立申請程序，可經下列者開展：

（一）利害關係人本人；

（二）作為利害關係人的受權人且具開立帳戶代理權的自然人。

二、實體使用者帳戶的開立申請程序，可經下列者開展：

（一）作為實體的受權人且具開立帳戶代理權的自然人；

（二）作為第四條第二款（一）項規定的行政機關的自然人，或如屬合議機關時的該機關主席；

（三）作為第四條第二款（一）及（二）項規定的實體的法定代表或部門領導人，在行使本身職權、獲授予的職權或獲轉授的職權時的自然人；

（四）作為第四條第二款（三）至（五）項規定的實體的法定代表的自然人。

第十條

確認身份程序

一、確認身份程序包括取得由利害關係人聲明的身份資料所需的工作，當中包含證明身份的方法，尤其為核實證據方法的真確性和有效性而須進行的控制工作。

二、確認身份程序可針對下列目的而組織：

（一）確保所聲明的身份在使用者帳戶系統內是獨有的，以及所聲明身份所屬的自然人或實體在法律現實中客觀存在；

（二）實現上項規定的目的，並從一或多個合格來源去核實所聲明的身份資料，以便證實該身份為活躍使用者且屬自然人或實體所有；

（三）如屬自然人，則須實現（一）和（二）項規定的所有目的，並藉對比一個或多個身體特徵以當面核實利害關係人的身份。

第十一條

確認自然人的身份

一、為達至滿意級保障水平，確認自然人身份的程序應符合下列要素：

（一）如屬當面程序：

Artigo 9.º

Apresentação do pedido de abertura

1. O processo do pedido de abertura de conta de utilizador de pessoa singular pode ser iniciado por:

1) O próprio interessado;

2) Pessoa singular que actue como procurador do interessado, com poderes de representação para abertura de conta.

2. O processo do pedido de abertura de conta de utilizador de entidade pode ser iniciado por:

1) Pessoa singular que actue como procurador da entidade, com poderes de representação para abertura de conta;

2) Pessoa singular que constitui órgão administrativo previsto na alínea 1) do n.º 2 do artigo 4.º ou, no caso de órgão colegial, o presidente desse órgão administrativo;

3) Pessoa singular que é representante legal de entidade ou que é dirigente de serviço previstos nas alíneas 1) e 2) do n.º 2 do artigo 4.º, no exercício de competências próprias, delegadas ou subdelegadas;

4) Pessoa singular que é representante legal de entidade prevista nas alíneas 3) a 5) do n.º 2 do artigo 4.º

Artigo 10.º

Processo de confirmação da identidade

1. O processo de confirmação da identidade abrange as acções necessárias para obter informação sobre a identidade declarada pelo interessado, incluindo meios de prova dessa identidade, e as acções necessárias para controlar esses meios de prova, nomeadamente para verificar se são genuínos e válidos.

2. O processo de confirmação da identidade pode ser organizado com os seguintes objectivos:

1) Assegurar que a identidade declarada é única no contexto desse sistema de conta de utilizador e assegurar que a pessoa singular ou entidade a quem pertence a identidade declarada existe objectivamente na realidade jurídica;

2) Satisfazer os objectivos previstos na alínea anterior e verificar a informação da identidade declarada junto de uma ou mais fontes qualificadas, para comprovar que essa identidade está activa e pertence à pessoa singular ou entidade;

3) No caso de pessoas singulares, satisfazer todos os objectivos previstos nas alíneas 1) e 2) e verificar presencialmente a identidade do interessado, através da comparação de uma ou mais características físicas.

Artigo 11.º

Confirmação da identidade de certa pessoa singular

1. Para alcançar o nível de garantia satisfatório, no processo de confirmação da identidade de certa pessoa singular devem ser cumpridos os seguintes elementos:

1) Quando o processo seja realizado presencialmente:

（1）確保利害關係人持有由合格來源發出的、附有證件獲發人相片的身份證明文件；

（2）核實所遞交的身份證明文件應屬真確，並以文件上的日期核實其仍在有效期內。

（二） 如屬遙距程序：

（1）利害關係人應發送證明以證其持有由合格來源發出的、附有證件獲發人相片的身份證明文件，例如居民身份證、護照、駕駛執照等的數碼副本；

（2）核實收到副本的身份證明文件應屬真確，並以文件上的日期核實其仍在有效期內。

二、為達至高級保障水平，確認自然人身份的程序應符合上款規定的要素及下列所有要素：

（一）如屬當面程序：

（1）確認利害關係人所遞交的身份證明文件的法律狀況，在可能時向發件的合格來源查詢；

（2）確定利害關係人知悉可能只有由所聲明身份所屬的人才知悉的資料或採取等同措施以減低利害關係人不具所聲明身份的風險，尤須考慮所遞交的是丟失、被盜、已中止、已廢止或失效的證據資料等風險。

（二）如屬遙距程序：

（1）確保利害關係人持有一種具合格來源的高級或更高的保障水平的電子身份識別工具；

（2）保證透過合格來源核實上一分項規定的電子身份識別工具的有效性；

（3）遵守上項（2）分項的規定。

三、為達至非常高級保障水平，確認自然人身份的程序應當面進行並符合下列要素：

（一）如利害關係人持有由澳門特別行政區內的合格來源發出的、附有證件獲發人相片或生物識別資料的身份證明文件，則須確保符合第一款（一）項和第二款（一）項規定的所有要素，並確保藉對比一個或多個身體特徵以核實利害關係人的身份；

（二）如利害關係人未持有上項規定的文件，則須確保符合第一款（一）項和第二款（一）項規定的所有要素，並確保藉收集包括利害關係人的相片或生物識別資料等身份資料來識別其身份。

(1) Assegurar que o interessado está na posse de um documento de identificação, emitido por fonte qualificada, com fotografia da pessoa a quem esse documento foi emitido;

(2) Verificar que o documento de identificação apresentado parece genuíno e está dentro do período de validade, de acordo com as datas nele indicadas;

2) Quando o processo seja realizado à distância:

(1) O interessado deve enviar prova que está na posse de um documento de identificação, emitido por fonte qualificada, com fotografia da pessoa a quem esse documento foi emitido, nomeadamente cópia digital do BIR, do passaporte, da carta de condução;

(2) Verificar que o documento de identificação cuja cópia se recebeu parece genuíno e está dentro do período de validade, de acordo com as datas nele indicadas.

2. Para alcançar o nível de garantia elevado, no processo de confirmação da identidade de certa pessoa singular devem ser cumpridos os elementos previstos no número anterior e todos os seguintes elementos:

1) Quando o processo seja realizado presencialmente:

(1) Confirmar a situação jurídica do documento de identificação apresentado pelo interessado, nomeadamente, se possível, por consulta à fonte qualificada que emitiu esse documento;

(2) Verificar que o interessado conhece informação que provavelmente só seria conhecida da pessoa a quem pertence a identidade declarada ou tomar medidas equivalentes para minimizar o risco de que a identidade do interessado não seja a identidade declarada, tendo em conta, nomeadamente, o risco de apresentação de elementos de prova perdidos, roubados, suspensos, revogados ou caducados;

2) Quando o processo seja realizado à distância:

(1) Assegurar que o interessado está na posse de um meio de identificação electrónica de nível de garantia elevado ou superior proveniente de fonte qualificada;

(2) Garantir a verificação, através de fonte qualificada, da validade do meio de identificação electrónica previsto na subalínea anterior;

(3) Cumprir o previsto na subalínea (2) da alínea anterior.

3. Para alcançar o nível de garantia muito elevado, o processo de confirmação da identidade de certa pessoa singular é realizado presencialmente e devem ser cumpridos os seguintes elementos:

1) Quando o interessado está na posse de um documento de identificação, emitido na RAEM por fonte qualificada, com fotografia ou dados biométricos da pessoa a quem esse documento foi emitido, assegurar que são cumpridos todos os elementos previstos na alínea 1) do n.º 1 e na alínea 1) do n.º 2 e, ainda, assegurar a verificação da identidade do interessado através da comparação de uma ou mais características físicas;

2) Quando o interessado não esteja na posse de documento previsto na alínea anterior, assegurar que são cumpridos todos os elementos previstos na alínea 1) do n.º 1 e na alínea 1) do n.º 2 e, ainda, assegurar a identificação do interessado através da recolha dos seus elementos de identificação, incluindo fotografia ou dados biométricos.

四、在公共部門或實體指定的地點內，由執行上級指派接待職務的工作人員進行的確認身份程序，或經由公共部門或實體的自動接待服務（自助服務機）進行的確認身份程序，視為當面確認身份程序。

第十二條

確認實體的身份

一、 為達至滿意級保障水平，確認實體身份的程序應符合下列要素：

（一）確保收集實體的身份資料，尤其商業名稱或名稱、法律性質的描述、住所及地點；

（二）在第四條第三款所規定的情況下，確保所收集的資料可識別及確定資訊設備；

（三）核實為證明（一）及（二）項規定的資料而遞交的文件應屬真確和有效。

二、為達至高級或更高的保障水平，確認實體身份的程序應符合下列要素：

（一）遵守上款（一）項，以及當適用時，（二）項的規定；

（二）確保對所遞交的文件作分析以確定其真確性；

（三）確保已採取措施以減低實體不具所聲明身份的風險，尤須考慮所遞交的是丟失、被盜、已中止、已廢止或失效的文件等風險；

（四）如法律規定屬相關類別的實體須將其存在和身份識別要素的資料予以登記或儲存，則須確定其法律狀況，在可能時向資料的合格來源查詢。

第十三條

帳戶的連接

一、經所有利害關係人同意，可將一個或多個自然人的電子身份識別工具與某一實體，包括其法定代表和工作人員的電子身份識別工具或使用者帳戶進行連接。

二、落實上款規定的連接，可讓實體的法定代表為身份識別工具已與實體連接的自然人界定不同的活動範圍。

4. Considera-se que o processo de confirmação da identidade é realizado presencialmente, quando o processo é realizado em local de atendimento indicado pelos serviços e entidades públicos, perante trabalhador dos serviços e entidades públicos superiormente designado para o atendimento, ou quando o processo é realizado em serviço de auto-atendimento (quiosque) dos serviços e entidades públicos.

Artigo 12.º

Confirmação da identidade de certa entidade

1. Para alcançar o nível de garantia satisfatório, no processo de confirmação da identidade de certa entidade devem ser cumpridos os seguintes elementos:

1) Assegurar que é recolhida informação de identificação da entidade, nomeadamente firma ou designação, descrição da natureza jurídica, sede e localização;

2) No caso previsto no n.º 3 do artigo 4.º, assegurar que é recolhida informação que permita individualizar e determinar o equipamento informático;

3) Verificar que os documentos apresentados para prova da informação prevista nas alíneas 1) e 2) parecem genuínos e válidos.

2. Para alcançar o nível de garantia elevado ou superior, no processo de confirmação da identidade de certa entidade devem ser cumpridos os seguintes elementos:

1) Cumprir o previsto na alínea 1) e, quando aplicável, na alínea 2) do número anterior;

2) Assegurar que os documentos apresentados são analisados para determinar a sua autenticidade;

3) Assegurar que foram aplicadas medidas para minimizar o risco de que a identidade da entidade não seja a identidade declarada, tendo em conta, nomeadamente, o risco de apresentação de documentos perdidos, roubados, suspensos, revogados ou caducados;

4) Quando seja legalmente exigido, para as entidades do tipo da entidade em causa, o registo ou o depósito da informação sobre a respectiva existência e os seus elementos de identificação, confirmar a sua situação jurídica, se possível por consulta à fonte qualificada para essa informação.

Artigo 13.º

Ligações entre contas

1. Podem ser estabelecidas, com o consentimento de todos os interessados, ligações entre os meios de identificação electrónica de uma ou mais pessoas singulares e os meios de identificação electrónica ou conta de utilizador de uma entidade, abrangendo, nomeadamente, os representantes legais e os trabalhadores dessa entidade.

2. As ligações previstas no número anterior podem ser concretizadas de modo que permita ao representante legal de determinada entidade definir âmbitos de actuação diferentes às pessoas singulares cujos meios de identificação electrónica ficam ligados a essa entidade.

三、為達至滿意級保障水平，第一款規定的連接應符合下列要素：

（一）確保自然人和實體為使用者帳戶持有人；

（二）確保核實自然人在擔任實體的法定代表或機關代表方面的權力，或核實實體的法定代表已獲許可作出連接；

（三）核實作為證明上項規定的資料而遞交的文件應屬真確和有效。

四、為達至高級或更高的保障水平，第一款規定的連接應符合下列要素：

（一）確保自然人和實體為使用者帳戶持有人；

（二）確保自然人和實體的身份確認程序達至高級或更高的保障水平；

（三） 符合上款（二）項規定的要素；

（四）確保對所遞交的文件的真確性作分析；

（五）如法律規定相關實體的代表須將擔任職務和其身份識別要素的資料予以登記或儲存，則須確定其法律狀況，在可能時向資料的合格來源查詢。

第十四條

紀錄

一、使用者帳戶系統應包含一個使用者帳戶的資訊紀錄，該紀錄應持續更新及受保護，以防止未經許可的修改，且應按照適用於電子政務和個人資料保護的法律及法規的規定來組織。

二、開立使用者帳戶階段的記錄程序，尤其包括對已收集應保存的文件、確認身份程序的資料、已建立連接的資料、在程序中已執行的措施及其結果的資料，以及其他相關要素作記錄。

第十五條

決定

一、根據上條第二款的規定完成記錄程序後，應立即因應個案的情況作出下列任一項合適的決定：

（一）中止申請，以便對收集的資料和相關的證明資料作深入分析，但中止期間不得超逾三十日且不得延期；

3. Para alcançar o nível de garantia satisfatório, a ligação prevista no n.º 1 deve cumprir os seguintes elementos:

1) Assegurar que a pessoa singular e a entidade são titulares de conta de utilizador;

2) Assegurar a verificação dos poderes da pessoa singular no âmbito da representação legal ou orgânica da entidade ou a verificação da existência de autorização do representante legal da entidade para a realização da ligação;

3) Verificar que os documentos apresentados para prova da informação prevista na alínea anterior parecem genuínos e válidos.

4. Para alcançar o nível de garantia elevado ou superior, a ligação prevista no n.º 1 deve cumprir os seguintes elementos:

1) Assegurar que a pessoa singular e a entidade são titulares de conta de utilizador;

2) Assegurar que os processos de confirmação da identidade da pessoa singular e da entidade alcançam o nível de garantia elevado ou superior;

3) Cumprir os elementos previstos na alínea 2) do número anterior;

4) Assegurar a análise da autenticidade dos documentos apresentados;

5) Quando seja legalmente exigido, para os representantes da entidade em causa, o registo ou o depósito da informação sobre o respectivo exercício de funções e os seus elementos de identificação, confirmar a sua situação jurídica, se possível por consulta à fonte qualificada para essa informação.

Artigo 14.º

Registo

1. O sistema de conta de utilizador deve incluir um registo informático das contas de utilizador, permanentemente actualizado, o qual deve ser protegido contra alterações não autorizadas e estar organizado em obervância das regras legais e regulamentares aplicáveis à governação electrónica e à protecção de dados pessoais.

2. O processo de registo da fase de abertura de conta de utilizador inclui, nomeadamente, o registo da documentação recolhida e que deva ser conservada, da informação sobre o processo de confirmação da identidade, sobre as ligações estabelecidas, sobre as diligências realizadas nos processos e respectivos resultados, e doutros elementos pertinentes.

Artigo 15.º

Decisão

1. Concluído o processo de registo previsto no n.º 2 do artigo anterior, deve ser imediatamente tomada decisão adequada às circunstâncias do caso, num dos seguintes sentidos:

1) Suspensão do pedido, por prazo de não superior a 30 dias improrrogável, para análise aprofundada da informação recolhida e dos respectivos elementos de prova;

（二）批准帳戶開立申請。

二、如屬中止申請的情況，應在上款（一）項規定的限期內將最終決定通知利害關係人。

三、上款規定經作出必要配合後適用於帳戶連接的申請。

第三章
電子身份識別工具的管理階段

第十六條
電子身份識別工具管理階段的範圍

一、電子身份識別工具的管理階段，包含電子身份識別工具生命周期的各個相關程序，尤其下列所有或某些程序：

（一）電子身份識別工具的生成，包括電子身份識別工具的預備、個人化、初始化和扣聯程序；

（二）電子身份識別工具的遞交；

（三）電子身份識別工具的啟動；

（四）電子身份識別工具的儲存和看管；

（五）電子身份識別工具的中止、廢止和重新啟動；

（六）電子身份識別工具的續期和替換。

二、上款規定的各個程序可全部由使用者帳戶系統的責任實體執行，或由參與生成使用者帳戶系統電子身份識別工具的多個實體協同執行。

三、在執行第十四條第一款的規定時，電子身份識別工具管理階段的記錄程序，尤其包括對每一電子身份識別工具的活動歷程以及相關情況或現狀作記錄。

四、每一電子身份識別工具的活動紀錄，僅因維護、審計和調查保安漏洞所需時方予保留和保護，其後須以安全方式銷毀。

第十七條
電子身份識別工具的特徵

一、使用者帳戶系統可將不同的電子身份識別工具與一個使用者帳戶扣聯，各電子身份識別工具可有不同特徵和保障水平。

二、為達至滿意級保障水平，電子身份識別工具應至少使用一個認證因素。

2) Deferimento do pedido de abertura de conta de utilizador.

2. No caso de suspensão do pedido, a decisão final deve ser comunicada ao interessado até ao termo do prazo previsto na alínea 1) do número anterior.

3. O disposto no número anterior é aplicável, com as necessárias adaptações, ao pedido de ligação entre contas.

CAPÍTULO III
Fase de gestão dos meios de identificação electrónica

Artigo 16.º
Âmbito da fase de gestão dos meios de identificação electrónica

1. A fase de gestão dos meios de identificação electrónica compreende os processos relativos ao ciclo de vida de um meio de identificação electrónica, nomeadamente todos ou alguns dos seguintes processos:

1) Produção do meio de identificação electrónica, incluindo processos de preparação, personalização, inicialização e vinculação do meio de identificação electrónico;

2) Entrega do meio de identificação electrónica;

3) Activação do meio de identificação electrónica;

4) Depósito e guarda do meio de identificação electrónica;

5) Suspensão, revogação e reactivação do meio de identificação electrónica;

6) Renovação e substituição do meio de identificação electrónica.

2. Os processos previstos no número anterior podem ser todos executados, na íntegra, pela entidade responsável pelo sistema de conta de utilizador ou ser executados de forma integrada por várias entidades que participem na produção dos meios de identificação electrónica desse sistema de conta de utilizador.

3. Em cumprimento do previsto no n.º 1 do artigo 14.º, o processo de registo da fase de gestão dos meios de identificação electrónica inclui, nomeadamente, o histórico das acções relativas a cada meio de identificação electrónica e a respectiva situação ou estado actual.

4. Os registos das acções relativas a cada meio de identificação electrónica são mantidos e protegidos somente enquanto forem necessários para fins de manutenção, de auditoria e de investigação de violações de segurança, devendo proceder-se depois à sua destruição de forma segura.

Artigo 17.º
Características dos meios de identificação electrónica

1. O sistema de conta de utilizador pode vincular vários meios de identificação electrónica a uma conta de utilizador, os quais podem ter características e níveis de garantia diferentes.

2. Para alcançar o nível de garantia satisfatório, um meio de identificação electrónico deve utilizar, pelo menos, um factor de autenticação.

三、為達至高級或更高的保障水平，電子身份識別工具應至少使用兩種不同的認證因素。

第十八條

電子身份識別工具的生成

一、為達至滿意級或高級保障水平，電子身份識別工具的生成應符合下列要素：

（一）使用格式化程序和文檔程序；

（二）在完成尤其是個人化或扣聯程序等生成程序之前，確保電子身份識別工具將與正確的使用者帳戶扣聯；

（三）當適用時，確保用作創設或裝載電子身份識別的裝置或設備須存於安全地方，以及備有一份持續更新的裝置或設備清冊，作為應對盜竊或企圖擅用等情況的保護措施。

二、為達至非常高級保障水平，電子身份識別工具的生成應符合上款規定的要素；如電子身份識別工具以裝置或設備裝載，尚應確保其於生成程序完結後處於上鎖狀態。

第十九條

電子身份識別工具的遞交和啟動

一、為達至滿意級保障水平，遞交和啟動電子身份識別工具應符合下列要素：

（一）使用格式化程序和文檔程序；

（二）電子身份識別工具發出後，須透過一個能推定該工具只會送達所屬的人或實體的機制或程序作遞交。

二、為達至高級保障水平，遞交和啟動電子身份識別工具應符合下列要素：

（一）使用格式化程序和文檔程序；

（二）電子身份識別工具發出後，須當面遞交或利用一個安全途徑由遞交對象以任何方式作出確認接收通知，以及利用能推定電子身份識別工具只會由所屬的人或實體持有的程序作遞交；

（三）確保採用例如答問式協議等措施，以減低電子身份識別工具於啟動時並非由其所屬的人或實體持有的風險。

3. Para alcançar o nível de garantia elevado ou superior, um meio de identificação electrónico deve utilizar, pelo menos, dois factores de autenticação de diferentes categorias.

Artigo 18.º

Produção dos meios de identificação electrónica

1. Para alcançar o nível de garantia satisfatório ou o nível de garantia elevado, na produção dos meios de identificação electrónica devem ser cumpridos os seguintes elementos:

1) Utilizar processos formalizados e documentados;

2) Assegurar, antes de finalizar os processos de produção, nomeadamente os processos de personalização ou vinculação, que o meio de identificação electrónica vai ficar vinculado à conta de utilizador correcta;

3) Assegurar, quando aplicável, que os dispositivos ou equipamentos utilizados para criar ou conter o meio de identificação electrónica estão guardados em local seguro e existe um inventário, permanentemente actualizado, desses dispositivos ou equipamentos que permite tomar medidas de protecção nos casos de roubo e de tentativa de uso não autorizado.

2. Para alcançar o nível de garantia muito elevado, na produção dos meios de identificação electrónica devem ser cumpridos os elementos previstos no número anterior e, no caso de meio de identificação electrónica contido em dispositivo ou equipamento, deve assegurar-se, ainda, que o meio de identificação electrónica é colocado, no final dos processos de produção, no estado de bloqueado.

Artigo 19.º

Entrega e activação dos meios de identificação electrónica

1. Para alcançar o nível de garantia satisfatório, na entrega e na activação dos meios de identificação electrónica devem ser cumpridos os seguintes elementos:

1) Utilizar processos formalizados e documentados;

2) Após a emissão, os meios de identificação electrónica são entregues através de um mecanismo ou de um procedimento que permite presumir que só chegam à pessoa ou entidade a que pertencem.

2. Para alcançar o nível de garantia elevado, na entrega e na activação dos meios de identificação electrónica devem ser cumpridos os seguintes elementos:

1) Utilizar processos formalizados e documentados;

2) Após a emissão, os meios de identificação electrónica são entregues presencialmente ou através de um canal seguro, com confirmação da recepção através de qualquer comunicação do destinatário nesse sentido, com procedimentos que permitem presumir que os meios de identificação electrónica só ficam na posse da pessoa ou entidade a que pertencem;

3) Assegurar a aplicação de medidas, nomeadamente protocolo baseado em pergunta–resposta, que permitam minimizar o risco de o meio de identificação electrónica não estar na posse da pessoa ou entidade a que pertence, no momento em que ocorre a respectiva activação.

三、為達至非常高級保障水平，遞交和啟動電子身份識別工具應符合上款（一）、（二）項規定的要素及下列要素：

（一）確保電子身份識別工具和電子身份識別工具的創設裝置，只能在該裝置所屬的人或實體持有時方可啟動；

（二）在執行上項規定時，所採用的程序須令電子身份識別工具只能在預定期限內啟動，以及能顯示啟動操作是由其持有者執行。

第二十條

電子身份識別工具的中止、廢止及重新啟動

一、使用者帳戶系統須確保符合下列要素：

（一）得以適時及有效的方式中止或廢止電子身份識別工具；

（二）已採取措施阻止未經許可的中止、廢止或重新啟動；

（三）電子身份識別工具僅在仍符合其中止或廢止之前所定的同樣保障水平要件時方能重新啟動。

二、上款的規定適用於所有保障水平。

第二十一條

續期及替換

一、電子身份識別工具的續期或替換程序應以擁有同級或較高級保障水平的有效電子身份識別工具為基礎。

二、如屬上款規定的情況，為達至非常高級保障水平，還須向一合格來源核實身份識別數據。

三、如欠缺第一款規定的有效電子身份識別工具，對電子身份識別工具的續期及替換程序適用經作出必要配合的第十條至第十二條的規定。

第四章

認證階段

第二十二條

認證階段範圍

一、認證階段包括目的為監控認證過程中，特別是認證時使用電子身份識別工具期間，可能出現的危險或威脅而由使用者帳戶系統展開的各項程序和措施。

3. Para alcançar o nível de garantia muito elevado, na entrega e na activação dos meios de identificação electrónica devem ser cumpridos os elementos previstos nas alíneas 1) e 2) do número anterior e, ainda, os seguintes elementos:

1) Assegurar que a activação do meio de identificação electrónica e a activação do dispositivo de criação do meio de identificação electrónica só ocorrem quando estão na posse da pessoa ou entidade a que pertencem;

2) Utilizar um procedimento, no cumprimento da alínea anterior, que permita a activação somente dentro de um prazo previamente definido e que permita demonstrar que as operações de activação foram executadas pelo titular do meio de identificação electrónica.

Artigo 20.º

Suspensão, revogação e reactivação dos meios de identificação electrónica

1. Devem estar assegurados, no sistema de conta de utilizador, os seguintes elementos:

1) É possível suspender ou revogar um meio de identificação electrónica de uma forma atempada e eficaz;

2) Foram tomadas medidas para impedir a suspensão, revogação ou reactivação não autorizadas;

3) A reactivação do meio de identificação electrónica só ocorre se os mesmos requisitos de nível de garantia estabelecidos antes da suspensão ou revogação continuarem a verificar-se.

2. O disposto no número anterior é aplicável a todos os níveis de garantia.

Artigo 21.º

Renovação e substituição

1. Os processos de renovação ou substituição de um meio de identificação electrónica devem basear-se na titularidade de um meio de identificação electrónica válido do mesmo nível de garantia ou superior.

2. Nos casos previstos no número anterior, para alcançar o nível de garantia muito elevado é necessário, ainda, verificar os dados de identificação junto de uma fonte qualificada.

3. Na falta do meio de identificação electrónica válido previsto no n.º 1, as disposições dos artigos 10.º a 12.º são aplicáveis, com as necessárias adaptações, nos processos de renovação e substituição dos meios de identificação electrónica.

CAPÍTULO IV

Fase de autenticação

Artigo 22.º

Âmbito da fase de autenticação

1. A fase de autenticação compreende os processos e as medidas que o sistema de conta de utilizador desenvolve para controlar os perigos ou ameaças potenciais nos procedimentos de autenticação, em especial durante o uso dos meios de identificação electrónica na autenticação.

二、上款所指的程序和措施應與認證所需的背景或環境以及已識別風險的程度相符。

第二十三條

程序及措施

在不妨礙執行數據格式、萬維網介面技術和電子郵件協議的互操作指引的情況下，上條第一款所指的程序及措施可主要包括：

（一）須使用具第十七條第三款規定的特徵的電子身份識別工具；

（二）須使用強密碼，尤其是沒有語義意義的合成字串；

（三）經一定次數嘗試輸入密碼失敗後，採用暫時的或需開解的上鎖機制；

（四）不得使用預設選項或默認選項的密碼，尤其是設備製造商的數據；

（五）對企圖在線破解密碼的失敗紀錄實施有系統的審計及分析程序，以便描繪該種在線攻擊的模式；

（六）使用具“hash”功能及“salt”值的密碼以阻止暴力破解密碼法（“brute-force attack”）的攻擊或預先計算好的“hashes”查找表（“rainbow table”）的攻擊；

（七）採取防假冒措施，尤其是支援證書裝置中的全息圖或微縮印；

（八）實施針對性的監控以檢測試圖獲取可識別個人身份資料的信息（“phishing”），包括停頓圖像的路線及來自不可靠來源的連結；

（九）採用互相認證機制和協議；

（十）採用認證機制和協議，惟該等機制和協議並不包括對網絡通訊密碼或在例外情況時需在網絡上對資料發出前的加密進行認證；

（十一）使用動態認證；

（十二）在信息中採用合格時間戳或等同方法；

（十三）使用實體的安全設備；

（十四）使用加密會話；

（十五）需輸入激活碼，尤其是PIN或屬性類別認證因素，以使用數字化證書；

（十六）以合格的來源核實數字化簽名，免受因下載未經授權修改的軟件所造成的影響；

2. Os processos e as medidas a que se refere o número anterior devem ser especificados em função da sua adequação ao contexto ou ambiente em que é exigida a autenticação e de forma proporcional aos riscos identificados.

Artigo 23.º

Processos e medidas

Sem prejuízo das instruções de interoperabilidade sobre formatos de dados, tecnologias de interface *Web* e protocolos de correio electrónico, os processos e as medidas a que se refere o n.º 1 do artigo anterior podem incluir, nomeadamente:

1) Necessidade de utilização de meio de identificação electrónica com as características previstas no n.º 3 do artigo 17.º;

2) Necessidade de utilização de senhas fortes, nomeadamente cadeias complexas sem significado semântico;

3) Aplicação de um mecanismo de bloqueio, temporário ou sujeito a acção de desbloqueio, após um certo número de tentativas fracassadas de introduzir uma senha;

4) Exclusão do uso de senhas predefinidas ou seleccionadas por defeito, nomeadamente dados do fabricante do dispositivo;

5) Implementação de procedimentos sistemáticos de auditoria e análise aos registos das tentativas fracassadas para construção de modelos descritivos dos ataques em linha para descobrir as senhas;

6) Uso de senhas com funções «*hash*» e valores «*salt*» para travar ataques de busca exaustiva das senhas («*brute-force attack*») ou ataques de tabela de consulta de «*hashes*» previamente calculados («*rainbow table*»);

7) Aplicação de medidas contra a falsificação, nomeadamente hologramas ou microimpressões, em dispositivos que funcionam com certificados;

8) Implementação de controlos desenvolvidos especificamente para detectar as mensagens que tentam obter informação pessoalmente identificável («*phishing*»), os quais incluem, nomeadamente, rotinas de desactivação de imagens e ligações provenientes de fontes não fiáveis;

9) Uso de mecanismos e protocolos de autenticação recíproca;

10) Uso de mecanismos e protocolos de autenticação que não incluam as senhas nas comunicações na rede ou, quando excepcionalmente seja necessário fazer a autenticação na rede, encriptação dos dados antes do envio;

11) Uso de autenticação dinâmica;

12) Aplicação de selos temporais qualificados ou método equivalente nas mensagens;

13) Uso de dispositivos físicos de segurança;

14) Uso de sessões encriptadas;

15) Necessidade de introdução de código de activação, nomeadamente um PIN ou um factor de autenticação intrínseco, para uso do certificado digital;

16) Verificação das assinaturas digitais através de uma fonte qualificada para contrariar os efeitos da descarga de *software* que tenha sido modificado sem autorização;

（十七）採用行動檢測技術和生命檢測技術，驗證是否存在以虛假的生物識別特徵企圖在屬性類別認證因素上作出的欺詐。

第二十四條

認證機制

一、認證機制為透過自然人或實體使用電子身份識別工具以證明其為工具的正當使用者。

二、為達至滿意級保障水平，認證機制應符合下列要素：

（一）在輸入個人身份識別資料之前，對電子身份識別工具及其有效性是否可靠作核實；

（二）如屬將個人身份識別資料儲存並使之成為認證機制的組成部分，所採用的安全措施須確保該等資料不會被丟失，更改或干擾，包括離線分析；

（三）執行安全監控，將具一般攻擊能力的、可尤其利用猜測活動、未經許可的監聽、複製或操作通信來破壞認證機制的入侵的可能性變為極度不可能。

三、為達至高級保障水平，認證機制應符合下列要素：

（一）在輸入個人身份識別資料之前，透過動態認證，尤其是一次性密碼，對電子身份識別工具及其有效性是否可靠作核實；

（二）如屬將個人身份識別資料儲存並使之成為認證機制的組成部分，須遵守上款（二）項的規定；

（三）執行安全監控，將具中度攻擊能力的、可尤其利用猜測活動、未經許可的監聽、複製或操作通信來破壞認證機制的入侵的可能性變為極度不可能。

四、為達至非常高級保障水平，認證機制應符合上款規定的要素，但上款（三）項規定的安全監控應符合將具高度攻擊能力的、可破壞認證機制的入侵的可能性變為極度不可能的要求。

第五章

系統的管理及組織

第二十五條

一般原則

一、使用者帳戶系統的責任實體以及第三條第二款所指的實體，應採取措施將提供予使用者的資訊作記錄、提供訊息安

17) Aplicação de técnicas de detecção de movimento e de detecção de vida para identificar tentativas de fraude a factor de autenticação intrínseco através de características biométricas artificiais.

Artigo 24.º

Mecanismo de autenticação

1. O mecanismo de autenticação consiste no método específico através do qual a pessoa singular ou a entidade utiliza o meio de identificação electrónica para demonstrar que é o respectivo utilizador legítimo.

2. Para alcançar o nível de garantia satisfatório, no mecanismo de autenticação devem ser cumpridos os seguintes elementos:

1) A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação electrónica e da sua validade;

2) Nos casos em que as informações de identificação pessoal ficam armazenadas e fazem parte do mecanismo de autenticação, as medidas de segurança aplicadas garantem que essas informações ficam protegidas contra perda, alteração ou interferência, incluindo análise *offline*;

3) Execução de controlos de segurança para tornar altamente improvável a possibilidade de um intruso com capacidade de ataque básica subverter o mecanismo de autenticação, nomeadamente através de actividades de adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações.

3. Para alcançar o nível de garantia elevado, no mecanismo de autenticação devem ser cumpridos os seguintes elementos:

1) A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação electrónica e da sua validade através de uma autenticação dinâmica, nomeadamente senha de uso único;

2) Nos casos em que as informações de identificação pessoal ficam armazenadas e fazem parte do mecanismo de autenticação, é cumprido o disposto na alínea 2) do número anterior;

3) Execução de controlos de segurança para tornar altamente improvável a possibilidade de um intruso com capacidade de ataque moderada subverter o mecanismo de autenticação, nomeadamente através de actividades de adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações.

4. Para alcançar o nível de garantia muito elevado, no mecanismo de autenticação devem ser cumpridos os elementos previstos no número anterior, mas os controlos de segurança previstos na alínea 3) do número anterior devem ser adequados a tornar altamente improvável a possibilidade de um intruso com capacidade de ataque elevada subverter o mecanismo de autenticação.

CAPÍTULO V

Gestão e organização do sistema

Artigo 25.º

Princípio geral

1. A entidade responsável pelo sistema de conta de utilizador e as entidades referidas no n.º 2 do artigo 3.º devem dispor de práticas documentadas de informações aos utilizadores, gestão de

全管理，以及按國際所認可的技術標準和良好慣例作出其他管控，以便顯示正在採用的方法是有效的並符合某一保障水平所針對的風險。

二、本規章的規定不得解作免除上款所指實體須遵守適用於相同事宜及事項的法律及法規的規定。

segurança da informação e de outros controlos implementados de acordo com as normas técnicas e as boas práticas internacionalmente reconhecidas, que permitam demonstrar que estão em vigor práticas eficazes e proporcionais aos riscos considerados em determinado nível de garantia.

2. As disposições do presente regulamento não podem ser interpretadas com o sentido de dispensar as entidades referidas no número anterior da observância das normas legais e regulamentares aplicáveis às mesmas matérias ou assuntos.

第二十六條

向使用者提供的資訊

一、使用者帳戶系統服務的取得及使用方法和條件的相關規則，應公開供利害關係人查閱。

二、應實施適當措施及程序，確保適時及以可靠方式讓服務使用者知悉任何關於上款所定規則的修改。

三、應實施適當措施及程序，以詳盡、準確以及與現有實際服務慣例和水平一致的方式回應信息的請求。

四、第一款至第三款的規定適用於所有級別的保障水平。

Artigo 26.º

Informações aos utilizadores

1. As regras sobre formas e condições de acesso e de utilização dos serviços do sistema de conta de utilizador devem estar publicamente disponíveis para consulta dos interessados.

2. Devem ser implementadas as medidas e procedimentos adequados a garantir que os utilizadores dos serviços são informados tempestivamente e de forma fiável de qualquer alteração às regras previstas no número anterior.

3. Devem ser implementadas as medidas e procedimentos adequados para que os pedidos de informação recebam respostas exaustivas, exactas e consistentes com as práticas e níveis de serviço efectivamente existentes.

4. O disposto nos n.os 1 a 3 é aplicável a todos os níveis de garantia.

第二十七條

信息安全管理

一、為達至滿意級保障水平，使用者帳戶系統應包括一個能有效管理及控制信息安全風險的信息安全管理系統。

二、為達至高級或更高的保障水平，使用者帳戶系統應包括一個符合上款規定的有效性要件並遵守技術標準或經證實的信息安全風險管理和控制原則的安全管理系統。

Artigo 27.º

Gestão da segurança da informação

1. Para alcançar o nível de garantia satisfatório, o sistema de conta de utilizador deve incluir um sistema de gestão da segurança da informação eficaz para a gestão e controlo dos riscos da segurança da informação.

2. Para alcançar o nível de garantia elevado ou superior, o sistema de conta de utilizador deve incluir um sistema de gestão da segurança que satisfaz o requisito de eficácia previsto no número anterior e respeita normas técnicas ou princípios comprovados de gestão e controlo dos riscos de segurança da informação.

第二十八條

設施及人員

為達至滿意級或更高的保障水平，第二十五條第一款所指實體須因應使用者帳戶系統所開展活動的風險程度遵守下列要件：

（一）設有能確保工作人員得到適當培訓並具備執行其所擔任職務所需能力的方法；

（二）用作提供使用者帳戶系統服務的設施須長期受監控，以便查察及防止環境現象所造成的損害、未經許可的進入以及其他可能影響部門安全的因素；

Artigo 28.º

Instalações e pessoal

Para alcançar o nível de garantia satisfatório ou superior, as entidades referidas no n.º 1 do artigo 25.º devem satisfazer, na medida proporcional aos riscos das actividades que desenvolvem no sistema de conta de utilizador, os seguintes requisitos:

1) Existem procedimentos que asseguram que os trabalhadores são devidamente formados e qualificados nas competências necessárias para executar as funções que desempenham;

2) As instalações utilizadas para prestar os serviços do sistema de conta de utilizador são permanentemente monitorizadas para detectar e proteger contra os danos causados por fenómenos ambientais, o acesso não autorizado e outros factores que possam afectar a segurança do serviço;

（三）用作提供使用者帳戶系統服務的設施須保證保存或處理個人資訊、加密資訊或其他敏感資訊的區域僅限於獲許可人士進入。

第二十九條

技術控制

一、為達至滿意級保障水平，使用者帳戶系統應確保下列要素：

（一）設有為管理與服務安全有關的風險及與所處理資料的保密性、完整性和可用性有關的風險而須提供的技術控制；

（二）用作收發個人或敏感資訊的電子通訊渠道應能防止被攔截、操作和複製；

（三）如生成或遞交電子身份識別工具的程序需使用敏感加密材料，獲取該材料時只能嚴格限於使用獲取所必需的功能及應用程式；

（四）實施能確保敏感加密材料絕對不會持續儲存於文本格式的程序；

（五）實施能保證安全性能長久維持，並有能力應對各級風險的變化、事件及安全漏洞的程序；

（六）所有包含加密數據、個人資料或其他敏感資料的載體須以安全方式存儲、傳輸和刪除。

二、為達至高級或更高的保障水平，應確保上款規定的要素，並須確保在生成或遞交電子身份識別工具程序及認證中所使用的敏感加密資料不被濫用。

第三十條

內部審計

使用者帳戶系統須定期作內部審計，包括對第二十五條第一款所指的所有實體，以便保證使用者帳戶系統的服務符合相關的要素及要件。

3) As instalações utilizadas para prestar os serviços do sistema de conta de utilizador garantem que o acesso às zonas de conservação ou tratamento de informações pessoais, criptográficas ou outras informações sensíveis é limitado a pessoas autorizadas.

Artigo 29.º

Controlos técnicos

1. Para alcançar o nível de garantia satisfatório, devem estar assegurados, no sistema de conta de utilizador, os seguintes elementos:

1) Existem controlos técnicos proporcionados para gerir os riscos relativos à segurança dos serviços e à confidencialidade, integridade e disponibilidade das informações tratadas;

2) Os canais de comunicação electrónicos utilizados para envio e recepção de informações pessoais ou sensíveis estão protegidos contra a intercepção, a manipulação e a reprodução;

3) Quando seja utilizado material criptográfico sensível em processo de produção ou de entrega de meio de identificação electrónica, o acesso a esse material está estritamente limitado às funções e aplicações que exijam esse acesso;

4) Estão implementados procedimentos que asseguram que o material criptográfico sensível nunca é armazenado de forma persistente em formato de texto;

5) Estão implementados 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;

6) Todos os suportes que contenham dados criptográficos, dados pessoais ou outros dados sensíveis são armazenados, transportados e eliminados de forma segura.

2. Para alcançar o nível de garantia elevado ou superior, devem estar assegurados os elementos previstos no número anterior e deve estar, ainda, assegurado que o material criptográfico sensível é protegido contra a manipulação abusiva, caso seja utilizado em processo de produção ou entrega de meio de identificação electrónica e na autenticação.

Artigo 30.º

Auditorias internas

São realizadas auditorias internas periódicas ao sistema de conta de utilizador, as quais são planeadas para incluir todas as entidades referidas no n.º 1 do artigo 25.º, a fim de garantir a conformidade dos serviços do sistema de conta de utilizador com os elementos e requisitos relevantes.

第 301/2018 號行政長官批示

行政長官行使《澳門特別行政區基本法》第五十條賦予的職權，並根據第35/2018號行政法規《電子服務》第十六條的規定，作出本批示。

一、核准附於本批示並為其組成部分的《統一電子平台使用者帳戶系統登入方式及條件規章》。

Despacho do Chefe do Executivo n.º 301/2018

Usando da faculdade conferida pelo artigo 50.º da Lei Básica da Região Administrativa Especial de Macau e nos termos do artigo 16.º do Regulamento Administrativo n.º 35/2018 (Serviços electrónicos), o Chefe do Executivo manda:

1. É aprovado o Regulamento sobre formas e condições de acesso ao sistema de conta de utilizador da plataforma electrónica uniformizada, anexo ao presente despacho e do qual faz parte integrante.