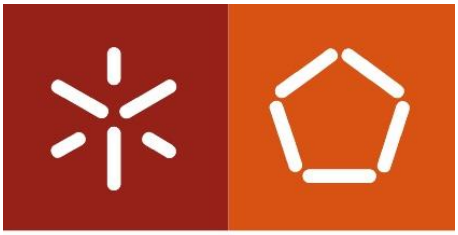

Universidade do Minho

Departamento de Informática

Mestrado em Engenharia Informática

Criptografia e Segurança de Informação

Engenharia de Segurança
Projeto de Análise - Sistema de identificação eletrónica

Grupo Nº 3

Ariana Lousada (PG47034) Luís Carneiro (PG46541)
Rui Cardoso (PG42849)

20 de março de 2022

Resumo

O presente documento descreve sucintamente os objetos de avaliação e de análise ao longo de um projeto de análise inserido na unidade curricular Engenharia de Segurança, pertencente ao perfil de Criptografia e Segurança da Informação inserido no Mestrado em Engenharia Informática da Universidade do Minho. Este projeto tem como alvo de análise um sistema de identificação eletrónica.

Conteúdo

Capítulo 1

Introdução

O projeto de análise descrito neste documento tem como principal objetivo avaliar o nível de garantia de cada uma das especificações técnicas e procedimentos elencados no anexo `CIR 2015/1502`, assim como o correspondente nível máximo de garantia que a autenticação no *homebanking* poderá ter.

Nesta análise em específico, escolheu-se o banco português Caixa Geral de Depósitos como entidade e a sua respetiva aplicação CaixaDireta como sistema de autenticação.

Uma vez que o grau de garantia a determinar é influenciado diretamente pela a implementação(ou não implementação) dos requisitos de nível de segurança que suportam o regulamento CIR, é necessário avaliar cada requisito individualmente, analisando simultaneamente a aplicação móvel da entidade em questão.

Este documento encontra-se dividido em quatro principais secções:

- Secção 2.1, na qual é classificado o fator de autenticação do sistema.
- Secção 2.2, na qual são abordados requisitos de registo e de gestão de modos de identificação eletrónica.
- Secção 2.3, na qual são abordados requisitos de segurança do mecanismo de autenticação.
- Secção 2.4, na qual são abordados os requisitos relacionados com a gestão e organização do sistema de autenticação.

Capítulo 2

Análise

2.1 Classificação do fator de autenticação

Um fator de autenticação consiste num fator pertencente a um utilizador que pode ser um destes tipos:

- *Fator de autenticação baseado no conhecimento*:

  Este tipo de fator requer conhecimento por parte do seu dono para verificação da sua identidade, como por exemplo *PINs* e *passwords*.

- *Fator de autenticação baseado na posse*:

  Este tipo de fator baseia-se num objeto físico pertencente ao seu dono. Podem por exemplo consistir em chaves privadas criptográficas armazenadas num determinado dispositivo de *hardware*, como os *smartcards*.

- *Fator de autenticação inerente*:

  Este tipo de fator baseia-se numa determinada característica física pertencente ao seu dono. Para autenticação é necessária a leitura e verificação por parte de um sistema desta característica, que pode ser por exemplo impressões digitais, íris, etc.

Estes três tipos de fatores podem também ser combinados para gerar uma autenticação *multi-factor*.

Os fatores de autenticação que são utilizados na aplicação CaixaDireta correspondem ao número de contrato, único para cada utilizador e respetiva palavra passe; ambos são do tipo *Knowledge-based*, visto que são credenciais que o utilizador deve conhecer de modo a ser capaz de efetuar a verificação de identidade na aplicação.

2.2 Especificações técnicas e procedimentos

2.2.1 Registo (Enrolment)

Ao longo desta secção serão abordados requisitos de aplicação, registo e de prova e verificação de identidade do utilizador que são necessários aquando da utilização do regulamento eIDAS.

Pedido e Registo

1. Assegurar que o requerente tem conhecimento dos termos e condições relacionados com a utilização dos meios de identificação eletrónica.

Esta informação pode ser consultada a qualquer momento na aplicação. A aplicação contém acesso ao website do banco Caixa Geral de Depósitos, no qual todos os pontos pertencentes aos termos e condições de uso estão inseridos publicamente.

Estes termos são apresentados ao utilizador no momento de registo na aplicação. O utilizador deve explicitamente aceitar estes termos para concluir o seu registo.

Para além disto, ao consultar a Cláusula 13ª das `Condições Gerais do Caixadirecta Empresas` verifica-se que a lei nacional se aplica.

2. Assegurar que o requerente tem conhecimento das precauções recomendadas relativamente à utilização dos meios de identificação eletrónica.

Esta informação também pode ser consultada a qualquer momento na aplicação, através de uma hiperligação para a secção de "Segurança e Fraude", na qual o utilizador pode se informar de vários tipos de recomendações de segurança, nomeadamente de *Internet Banking*, utilização de cartões, mecanismos CGD e de prevenção de fraudes, como por exemplo o *Phishing*.

Todo o tipo de recomendações encontra-se disponibilizado publicamente, como a deteção de casos de Phishing, concelhos na manutenção de cartões multibanco, em que dispositivos não se deve utilizar a aplicação, entre outros.

3. Recolher os dados de identificação necessários para a prova e verificação da identidade.

No processo de adesão à aplicação CaixaDireta, o utilizador deve inserir o seu número de contribuinte e de telemóvel, foto de cada face do seu documento de identificação(que neste caso será o cartão de cidadão) e ainda um "vídeo selfie"no qual o utilizador grava um vídeo de curta duração a expor o seu rosto[1]. Estes dados são depois validados utilizando uma fonte autorizada adequada.

Após a validação dos dados anteriormente referidos, o utilizador deve ativar explicitamente o serviço CaixaDireta e inserir o seu email pessoal para receber o seu número de contrato. Por fim, o utilizador tem acesso e aceita as condições do serviço, escolhendo também um código de acesso.

Este código de acesso, juntamente com o número de contrato são os principais dados que permitem a verificação da entidade do cliente sempre que quiser aceder ao serviço da aplicação CaixaDireta.

Nível de garantia

Uma vez que neste caso os elementos necessários mantêm-se para cada nível de garantia e que são os três implementados, podemos concluir que em termos de Pedido e Registo tem-se um nível de garantia elevado.

Prova e verificação da identidade (pessoa singular)

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.

Todo o utilizador da aplicação CaixaDireta possui um número de contrato e código de acesso a ele

[1]Estes fatores de tipo inerente apenas são requisitados no processo de registo. São utilizados sempre que se pretende validar o número de contrato no uso futuro da mesma conta de cliente.

associados. Estas "credenciais"podem ser validadas através de uma fonte autorizada que contenha outras informações referentes ao indivíduo inseridas no momento de registo. Neste caso, esta informação(prova) encontra-se em formato digital.

2. Pode considerar-se que os elementos de prova são genuínos, ou que são conformes com uma fonte qualificada e parecem ser válidos.

No sistema de autenticação em questão, as credenciais que o utilizador possui são validadas com o auxílio de *cross-validation* entre estas e os dados inseridos no momento de registo.

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.

A fonte autorizada neste caso, de modo a verificar se a conta existe no sistema e que se trata do utilizador, faz *cross-validation* dos dados inseridos no momento do registo (como por exemplo o "vídeo selfie") com os dados do utilizador.

4. 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; - Substancial, ponto 2

A fonte autorizada neste caso, de modo a verificar se a conta existe no sistema e que se trata do utilizador, faz *cross-validation* dos dados inseridos no momento do registo (como por exemplo o "vídeo selfie") com os dados do utilizador.

A inserção de evidência fotográfica do documento de identificação e do rosto do utilizador ajuda a minimizar riscos de entidade falsa e de informação desatualizada.

5. 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; - Elevado(1a)

Tal como já foi mencionado anteriormente, a CaixaDireta contém nas suas bases de dados um "vídeo selfie"que possibilita a comparação de características físicas do indivíduo com um *register* de acordo com uma fonte autorizada.

Nível de garantia

Dado que todos os elementos necessários ao nível Reduzido são implementados, assim como os pertencentes à segunda alternativa do nível Substancial e ainda os pertencentes à primeira alternativa no ponto a) do nível Elevado, pode-se concluir que a Prova e Verificação da identidade para pessoas singulares tem um nível de garantia Elevado.

Prova e verificação da identidade (pessoa coletiva)

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.

No momento de adesão por parte da pessoa coletiva, é introduzido o código representante da empresa. Este código pode ser utilizado por uma fonte autoritativa de modo a validar a sua identidade.

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.

De modo a concluir o registo, é necessário por parte da pessoa coletiva inserir dados como o número de conta ou de cliente, nome da empresa, nome do utilizador, telefone de contacto, endereço de email e número de contribuinte. Se for necessário, é possível recorrer à validação do número de contribuinte por parte de uma fonte autorizada. Também se pode verificar o número de conta/cliente acedendo a um *register* pertencente à Caixa Geral de Depósitos.

3. A pessoa coletiva não é reconhecida por uma fonte qualificada com um estatuto que a impeça de atuar como pessoa coletiva.

Tal como referido anteriormente, a empresa é registada com o respetivo código de empresa. Durante todo o processo de adesão a pessoa coletiva não sofre qualquer mudança de estatuto.

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, 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. - Substancial(3)

Ao consultar as condições gerais do CaixaDireta Empresas, especificamente a cláusula 6ª retira-se : "Os elementos de identificação referidos nos números anteriores serão atribuídos ao titular no ato de adesão ao serviço ou, sempre que a Caixa entender que se justifique, em momento posterior."

Estes elementos de identificação correspondem à Matriz e Hard Token que são gerados após ativação do contrato. São estes elementos que autorizam o acesso da pessoa coletiva ao serviço da CaixaDireta. Normalmente, estes elementos são gerados uma única vez após o ato de registo.

Nível de garantia

Uma vez que todos os elementos necessários pertencentes ao nível Reduzido são implementados juntamente com a terceira alternativa do nível Substancial, pode-se concluir que a Prova e verificação da identidade (pessoa coletiva) possui um nível de garantia Substancial.

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

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.

Cada conta de uma pessoa coletiva pode ser acedida por várias entidades pertencentes à empresa: Autorizador, Operador e Supervisor. Cada uma destas entidades corresponde a uma pessoa singular. Como já foi analisado na secção 2.2.1, a prova da identidade deste tipo de entidades tem um nível de garantia Elevado.

2. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional.

Nas Condições Gerais do serviço da CaixaDireta Empresas, ao consultar a cláusula 13ª pode-se retirar: "O presente contrato rege-se pela Lei portuguesa.".

3. A pessoa singular não é reconhecida por uma fonte qualificada com um estatuto que a impeça de agir em nome da pessoa coletiva.

Como já mencionado anteriormente, a pessoa coletiva está diretamente relacionada com várias entidades do tipo singular. Se a pessoa singular for um Autorizador, Operador ou Supervisor e tiver o acesso adequado, esta pode agir em nome da pessoa coletiva.

4. 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. - Substancial(1)

Analisado na secção 2.2.1 pode-se afirmar que a prova de identidade da pessoa singular é de nível de garantia Elevado.

5. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional, o que resultou na inscrição da ligação numa fonte qualificada. - Substancial(2)

Nas Condições Gerais do serviço da CaixaDireta Empresas, não se encontra qualquer referência a partir da qual se possa inferir que a ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional.

6. A ligação foi verificada com base nas informações provenientes de uma fonte qualificada. - Substancial(3).

Nas Condições Gerais do serviço da CaixaDireta Empresas, não se encontra qualquer referência a partir da qual se possa inferir que a ligação foi verificada com base nas informações provenientes de uma fonte qualificada.

7. 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. - Elevado(1)

Como objeto de análise já abordado na secção 2.2.1 pode-se afirmar que a prova de identidade da pessoa singular é de nível de garantia Elevado, portanto este ponto é implementado.

8. 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. - Elevado(2)

Uma vez que no momento de adesão a empresa insere o seu número de identificação, assim como o número de contribuinte, estes acabam por representar a pessoa coletiva num contexto nacional. Relativamente à pessoa singular associada, esta também é verificada utilizando os dados inseridos no momento e registo.

Nível de Garantia

Apesar todos os elementos necessários de nível Reduzido e Elevado implementados, o segundo ponto do nível Substancial não é cumprido.

Visto que para ter um nível de garantia Elevado seria necessário a implementação do ponto 3 do nível Reduzido, do ponto 2 do nível Substancial e dos pontos pertencentes ao nível Elevado, tem-se um nível de garantia Reduzido para a Ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas, devido à falha do segundo ponto do nível Substancial.

2.2.2 Gestão de modos de identificação eletrónica

Nesta secção será feita uma classificação de vários aspetos relacionados à gestão da identificação eletrónica, nomeadamente das suas caraterísticas e configuração, emissão, entrega e ativação, suspensão, revogação e ativação e, finalmente, da sua renovação e substituição.

Características e configuração dos meios de identificação eletrónica

1. Os meios de identificação eletrónica utilizam, pelo menos, um fator de autenticação.

De modo a autenticar um utilizador no portal do serviço CaixaDireita, apenas é preciso indicar o número do contrato e o respetivo código (que contém 6 dígitos). Ou seja, apenas 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.

Esta verificação não é feita. Tal como descrito na clásula 6ª, "Cada Utilizador terá elementos de acesso pessoais e intransmissíveis, que permitem, nomeadamente, a sua identificação, aquando da utilização do serviço, devendo os mesmos ser do seu exclusivo conhecimento e sendo a eventual utilização dos mesmos por terceiros imputável ao respetivo Utilizador...". A responsabilidade da utilização única deste serviço por parte do utilizador é exclusiva ao mesmo (esta clásula até obriga o utilizador a informar o banco Caixa Geral de Depósitos caso exista algum acesso indevido à sua conta por terceiros).

Nível de garantia

Estes dois requisitos perfazem o nível reduzido de garantia. Sendo que já o segundo requisito não é cumprido, não faz sentido percorrer os restantes níveis mais fortes de garantia.

Emissão, entrega e ativação

1. 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.

É possível ativar o serviço CaixaDireta de várias formas, quer seja pela aplicação CaixaDireta, no website ou até no ATM. A confirmação dada ao utilizador quando adere com sucesso a este serviço é presencial no caso da ATM, ao passo que tanto no site como na app esta é feita através do dispositivo usado, quer por SMS quer por e-mail.

Nível de garantia

Escolhendo as alternativas mais fracas - aplicação e website - a confirmação é entregue via SMS ou e-mail. Ora, estes meios de comunicação não garantem de todo que chegam só à pessoa que se destinam pois não é possível assumir que o número de telefone ou e-mail utilizado na adesão continua na posse do mesmo utilizador quando esta é terminada (por exemplo, o endereço de e-mail pode entretanto ter sido hackeado). Portanto, conclui-se que o nível baixo não foi atingido pelas razões mencionadas acima.

Suspensão, revogação e reativação

1. É possível suspender e/ou revogar um meio de identificação eletrónica de uma forma atempada e eficaz.

Esta condição verifica-se pois é possível retirar do dispositivo à escolha (telemóvel ou computador) o acesso online ao serviço caixadireta através do mesmo.

2. Foram tomadas medidas para impedir a sua revogação, suspensão e/ou reativação não autorizadas.

As medidas tomadas são as mesmas necessárias para aceder ao serviço caixadireta - conhecimento do número do contrato e respetivo código.

3. A reativação só terá lugar se os mesmos requisitos de garantia estabelecidos antes da suspensão ou revogação continuarem a verificar-se.

Todos os requisitos de garantia estabelecidos antes da suspensão ou revogação mantêm-se, pois os documentos necessários para ativar o serviço, em princípio, mantiveram-se iguais desde a suspensão ou revogação.

Nível de garantia

Todos estes elementos são cumpridos, pelo que o nível de garantia é ELEVADO.

Renovação e substituição

1. 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.

Tal como descrito em 4, para atualizar os dados pessoais, os clientes da CaixaDireta têm a possibilidade de comunicar com a Caixa Geral de Depósitos através da mesma plataforma. Para fazê-lo, têm que estar na sua conta, o que cumpre os mesmos requisitos de garantia do processo inicial de prova e verificação da sua identidade.

2. 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.

É possível anexar vários documentos de identificação eletrónica, como por exemplo o cartão de cidadão ou o comprovativo da morada. Apesar de não confirmado, é (razoavelmente) esperado que estes documentos sejam validados por parte do banco, pois os riscos de um utilizador assumir uma identidade diferente possivelmente com intenções de fraude seria devastador para a empresa.

Nível de garantia

Sendo assim, o nível de garantia é elevado visto o serviço cumprir todos os requisitos acima estabelecidos.

2.3 Autenticação

Nesta secção será discutido a segurança do mecanismo de autenticação.

Mecanismo de autenticação

1. A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação eletrónica e da sua validade.

Visto que o sistema discutido pertence a um banco, este é o requisito mínimo que este tem de assegurar (e assegura); a verificação feita deve possibilitar o acesso à conta do utilizador a que pertence apenas.

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.

É assumido que, dada a sensibilidade dos dados guardados, que todos estes são cifrados de modo a estarem protegidas caso ocorra perda e/ou fuga de dados.

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.

Esta condição também pode ser assumida pois existe um limite no número de tentativas para autenticação para combater a adivinhação e a tentativa de subverção dos mecanismos de autenticação. A escuta é inútil visto que todo o tráfego é cifrado. Finalmente, a reprodução dos pedidos é inviabilizada pelo uso de tokens e mecanismos de deteção do mesmo.

4. 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.

Já este requisito não é cumprido, visto que a autenticação, descrita na secção 2.2.1, é feita através de um fator baseado apenas no conhecimento - número de contrato e respetivo código.

Nível de garantia

Considerando todos estes requisitos, o nível de garantia atingido é reduzido, visto que apesar deste serviço apresentar alguns mecanismos de autenticação, a autenticação não é dinâmica.

2.4 Gestão e Organização

Nesta ultima secção são tidas em conta as disposições gerais, publicação de notificações e informações para os utilizadores, manutenção de registos, instalações e pessoal, controlos técnicos e conformidade e auditoria de acordo com o regulamento eIDAS.

Disposições gerais

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.

A caixa geral de depósitos é uma entidade pública empresarial.[2]

[2] https://st16direitoadministrativo.blogs.sapo.pt/a-caixa-geral-de-depositos-como-8535

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.

A partir de 25 de maio de 2018, passou a aplicar-se um novo Regulamento Geral de Proteção de Dados Pessoais. Desde então a Caixa Geral de Depósitos indica que segue o regulamento geral sobre a proteção de dados (RGPD). Toda esta informação pode ser consultada no ponto 4 das Referências(4).

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.

Este ponto pode ser confirmado na seguinte secção do *website* da caixa geral de depósitos: https://www.cgd.pt/Institucional/Noticias/Pages/Caixa-obtem-Certificacao-do-Sistema-de-Gestao-da-Continuidade-de-Negocio.aspx

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.

Os prestadores são responsáveis pelo cumprimento dos compromissos subcontratados a outra entidade. É importante que sejam apresentadas garantias que assegurem que o tratamento cumprirá as normas do RGPD.

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..

A Caixa Geral de Depósitos através das suas condições gerais de abertura de conta e prestação de serviços informa todas as pessoas singulares acerca dos serviços prestados. Pode ser consultado em: https://www.cgd.pt/_layouts/15/CaixatecCGDLayoutsV2/cgu.aspx?mod=207

Nível de garantia

Uma vez que todos os elementos necessários são implementados, as Disposições Gerais do sistema de autenticação possuem um nível de garantia Elevado.

Publicação de notificações e informações para os utilizadores

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.

Toda esta informação pode ser consultada online e em todos os balcões da caixa geral de depósitos. A entidade também possui uma política de protecção de privacidade de acordo com o GDPR.

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.

A actualização das condições de quaisquer serviços ou da politica de protecção da privacidade são informados ao cliente através do website da caixa geral e/ou através de email podendo também ser em

formato papel.

3. Devem ser postas em vigor políticas e procedimentos adequados para que os pedidos de informações recebam respostas exaustivas e exatas.

Existe uma secção "FAQ"onde se pode obter de forma rápida e fácil informações para determinadas questões. Para além disto a entidade pode ser contactada via e-mail, por uma linha telefónica aberta 24 horas todos os dias do ano para clientes particulares e das 8h as 22h para clientes empresa. Também é possível o atendimento presencial em balcão.

Nível de garantia

Uma vez que todos os elementos necessários são implementados, a Publicação de notificações e informações para os utilizadores do sistema de autenticação possui um nível de garantia Elevado.

Gestão da segurança da informação

1. Existe um sistema de gestão da segurança da informação eficaz para a gestão e controlo dos riscos da segurança da informação.

A Caixa Geral de Depósitos possui mecanismos de segurança através de tecnologia avançada, que utiliza vários mecanismos de teste de validade referidos já na secção 2.2.1.

2. O sistema de gestão da segurança das informações respeita normas ou princípios comprovados de gestão e controlo dos riscos de segurança da informação.

A CGD utiliza mecanismos de segurança que podem ser consultados em : https://www.cgd.pt/Ajuda/Seguranca/Pages/Mecanismos-de-seguranca.aspx

Nível de garantia

Uma vez que todos os elementos necessários são implementados, a Gestão da segurança da informação do sistema de autenticação possui um nível de garantia Elevado.

Manutenção de registos

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.

Toda a informação é guardada e processada de acordo com o GDPR.

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.

Toda a informação é guardada e processada de acordo com o GDPR.

Nível de garantia

Uma vez que todos os elementos necessários são implementados, a Manutenção de registos do sistema de autenticação possui um nível de garantia Elevado.

Instalações e pessoal

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

A contratação de pessoal é feita através de uma rigorosa selecção de candidatos e posteriormente caso necessário formação para garantir que estão qualificados para o cargo.Os candidatos podem aceder "A minha caixa"e preencher o formulário apresentado.

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.

Ao longo dos anos a caixa geral de deposito tem reduzido trabalhadores devido a sua recapitalização e plano de reestruturação.Em 2018 já tinham saído 7675 funcionários da empresa. Tendo isto em conta e as reviews do thrustpilot as pessoas queixam-se do atendimento. [3]

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.

A caixa geral de depósitos tenta que as suas instalações sejam o mais seguras possíveis. Realizam através do seu gabinete de protecção e segurança simulacros que são acompanhados por observadores/avaliadores externos e internos que analisam os procedimentos de segurança dos colaboradores e meios que a CGD dispõe. Estão preparadas para protecção contra corte de corrente através de UPS e geradores. O acesso a alguns balcões de atendimento requer o uso de cartão da cgd. Também possuem múltiplas câmaras de vigilância.

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

Os colaboradores apenas têm acesso a informação necessária para efectuar o seu trabalho. A informação sensível é cifrada e/ou limitada a colaboradores autorizados.

Nível de garantia

Visto que existem algumas queixas relativas ao atendimento por número insuficiente de contratantes, o segundo ponto não é implementado. Com isto, o nível reduzido de garantia não é alcançado.

Controlos técnicos

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.

A Caixa Geral de Depósitos adota várias medidas de segurança de carácter técnico e organizativo, de forma a proteger os dados pessoais dos seus clientes contra a perda, difusão, alteração, tratamento ou acesso indevidos ou não autorizados.

A conservação dos dados pode ser efetuada pelo período em que subsistirem obrigações legais ou

[3]

- https://www.rtp.pt/noticias/economia/cgd-reduziu-numero-de-trabalhadores-em-172-no-1o-semestre_n1163664
- https://pt.trustpilot.com/review/www.cgd.pt

decorrentes da relação comercial com os clientes.

2. Os canais de comunicação electrónicos utilizados para intercâmbio de informações sensíveis ou pessoais estão protegidos contra a interceção, a manipulação e a reprodução.

A informação partilhada através dos canais de comunicação electrónicos é protegida. O banco não pode prestar esclarecimentos relacionados com números de conta, saldos ou outras informações pessoais. A CGD tem dever de sigilo e de segurança de dados dos clientes.

3. O acesso a material criptográfico sensível, se utilizado para a emissão de meios de identificação electrónica 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.

A Caixa geral de depósitos através da criptografia protege o acesso aos sistemas e utiliza-a para codificar os dados guardados.

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.

A Caixa geral de Depósitos utiliza vários procedimentos para garantir a segurança de dados ao longo do tempo que facilmente são adaptáveis a novos riscos, incidentes e falhas de segurança: logout automático, utilização de certificados digitais, encriptação de comunicações, controlo de tráfego e monitorização de controlo.

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

Tal como referido anteriormente, o sistema de autenticação utiliza procedimentos como a encriptação de comunicações, que garantem a segurança durante o transporte de dados sensíveis. Os dados de cada cliente são também associados a uma matriz e a um Hard Token, o que evita a eliminação incorreta de dados importantes.

6. O material criptográfico sensível, se utilizado para a emissão de meios de identificação electrónica e a autenticação, é protegido contra a manipulação abusiva.

A Caixa geral de depósitos adota várias medidas de segurança de carácter técnico e organizativo, de forma a proteger os dados pessoais dos seus clientes contra a perda, difusão, alteração, tratamento ou acesso indevidos ou não autorizados. A conservação dos dados pode ser efetuada pelo período em que subsistirem obrigações legais ou decorrentes da relação comercial com os clientes.

Nível de garantia

Uma vez que todos os elementos necessários são implementados, os Controlos Técnicos do sistema de autenticação possuem um nível de garantia Elevado.

Conformidade e auditoria

1. 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.

Um dos objetos do Regulamento da Comissao de Auditoria de Controlo Interno da Caixa Geral de Depósitos garante este elemento: "A Comissão de Auditoria avalia, numa base anual, a suficiência da sua composição e organização."
Para além disto, uma das competências da Auditoria rege-se em "Zelar pela observância das disposições

legais e regulamentares, dos Estatutos e do Código de Conduta da Instituição, das normas e recomendações emitidas pelas autoridades de supervisão, bem como das políticas gerais, normas e práticas instituídas internamente".

2. 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.

Juntamente com os pontos abordados anteriormente, isto verifica-se com uma outra competência da auditoria: "Elaborar, numa base trimestral, o Relatório a remeter ao Ministério das Finanças, com a descrição dos controlos efetuados na sua atividade fiscalizadora, as anomalias e os principais desvios eventualmente detetados relativamente às previsões."

3. 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.

Compete à Comissão de Auditoria promover avaliações periódicas e independentes sobre a sua conduta e valores, a realizar por entidade externa e cumprir as demais atribuições constantes da Lei ou dos Estatutos.

4. Quando o regime é gerido diretamente por um organismo governamental, é objeto de uma auditoria realizada de acordo com o direito nacional.

Uma vez que a Caixa Geral de Depósitos se trata de uma entidade gerida pelo governo português, é possível ser alvo de uma auditoria realizada pelo próprio governo. [4]

Nível de garantia

Uma vez que todos os elementos necessários são implementados, a Conformidade e auditoria do sistema de autenticação possui um nível de garantia Elevado.

[4] https://www.publico.pt/2019/01/22/economia/noticia/cgd-auditoria-relatorio-faria-oliveira-1858870

Capítulo 3

Conclusão

Com a análise dos diferentes requisitos inseridos no CIR 2015/1502, de modo a obter o nível máximo possível de garantia do sistema de autenticação devem ser melhorados os seguintes pontos:

- Prova e verificação da identidade (pessoa coletiva) (2.1.3) : Nível de garantia substancial.
  É necessário implementar uma das três alternativas dos elementos necessários do nível Elevado de modo a melhorar este ponto.
- Ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas (2.1.4) : Nível de garantia reduzido.
  É necessário implementar o segundo elemento necessário pertencente ao nível Substancial. Visto que é o único ponto que falha, deste modo teria-se um nível de garantia Elevado.
- Características e configuração dos meios de identificação eletrónica (2.2.1): Sem nível de garantia.
  É necessário implementar o segundo ponto do nível Reduzido, de modo a ser possível melhorar as características e configuração dos meios de identificação eletrónica.
- Emissão, entrega e ativação (2.2.2) : Sem nível de garantia. É necessário alterar os meios de comunicação pelos quais são enviadas as confirmações de registo, uma vez que podem ser relativamente fáceis de manipular.
- Mecanismo de autenticação (2.3.1) : Nível de garantia reduzido.
  É necessário implementar autenticação dinâmica.
- Instalações e Pessoal (2.4.5) : Sem nível de garantia.
  É necessário empregar um maior número de subcontratantes de modo a melhorar o serviço ao cliente. Com isto este ponto teria um nível de garantia Elevado.

Capítulo 4

Referências

- https://github.com/uminho-mei-engseg-21-22/EngSeg/blob/main/Pratica2/Guidance_on_Levels_of_Assurance.docx
- https://www.cgd.pt/Empresas/Gestao_corrente/Servicos/Documents/Condicoes-Gerais-Servico-CDE.pdf
- https://www.cgd.pt/ajuda/Seguranca/Pages/Seguranca-e-Fraude.aspx
- https://www.youtube.com/watch?v=WN8jHxKQrjU
- https://www.anacom.pt/render.jsp?contentId=1371360
- https://www.cgd.pt/Empresas/Gestao_corrente/Servicos/Pages/Caixadirecta-empresas.aspx
- https://www.cgd.pt/Institucional/Noticias/Pages/Atualizar-Dados-Pessoais.aspx
- https://www.cgd.pt/Ajuda/Pages/Politica-de-Privacidade-e-Protecao-de-Dados-Pessoais.aspx
- https://www.cgd.pt/Site/Saldo-Positivo/Pages/Politica-de-privacidade.aspx
- https://www.cgd.pt/Institucional/Governo-Sociedade-CGD/Regulamentos/Documents/Regulamento-da-Comissao-Auditoria-Controlo-Interno.pdf