AT autoridade tributária e aduaneira

Plano de Ação AT

em matéria de reforço da segurança da informação, proteção de dados pessoais e confidencialidade fiscal

Plano de Ação AT

em matéria de reforço da segurança da informação,

proteção de dados pessoais e confidencialidade fiscal

Autoridade Tributária e Aduaneira – Ministério das Finanças

Classificação:

(Documento integra medidas aprovadas, em 19/06/2015, pelo Conselho de Administração da Autoridade Tributária e Aduaneira)

Rua da Prata nº 10
1149-027 Lisboa
URL: www.portaldasfinancas.gov.pt

ÍNDICE

I - INTRODUÇÃO

A Autoridade Tributária e Aduaneira (AT) foi objeto, no decurso do primeiro semestre de 2015, de auditorias por parte da Comissão Nacional de Proteção de Dados (CNPD) e da Inspeção Geral de Finanças (IGF) que incidiram sobre a verificação das regras implementadas em matéria de segurança informática e de observância das garantias de todos os contribuintes, no respeito pelo principio da igualdade.

Na sequência daquelas auditorias e das recomendações daí resultantes, o Senhor Secretário de Estado dos Assuntos Fiscais (SEAF) determinou, através do despacho nº. 105/2015-XIX, de 26 de maio de 2015, a apresentação pela AT de um plano de ação contendo medidas concretas e devidamente calendarizadas para dar cumprimento àquelas recomendações, devendo respeitar os seguintes princípios:

- A confidencialidade dos dados fiscais de cada contribuinte é um direito protegido pela Lei Geral Tributária, que materializa o direito à reserva da vida privada consagrado na Constituição da Republica Portuguesa, e que os utilizadores (internos e externos) são obrigados a proteger e salvaguardar;
- Na prossecução das funções que lhe estão confinadas, nomeadamente no que respeita à proteção do sigilo fiscal de todos os contribuintes, a AT está vinculada ao principio da legalidade e da igualdade, devendo por isso pautar a sua atuação por regras transparentes e devidamente fundamentadas, que se apliquem de forma igual a todos os contribuintes, não privilegiando uns em detrimento de outros;
- A devida proteção do sigilo fiscal de todos os contribuintes é uma prioridade para a administração fiscal, devendo ser reforçada a sua prossecução, designadamente através de metodologias conformes com os princípios legais e constitucionais em vigor.

Determinou ainda que o plano de ação deve incluir, entre outras, as seguintes linhas prioritárias de ação:

a. Proceder à revisão e reformulação do Plano de Segurança Informática da AT, com especial enfoque no reforço da proteção dos direitos dos contribuintes;
b. Rever, aperfeiçoar e comunicar os princípios e valores pelos quais se deve reger a atuação da AT, estabelecendo os mecanismos e os planos de formação que garantam o seu efetivo conhecimento e vinculação por parte de todos os seus funcionários, principalmente em matéria de proteção de dados pessoais;
c. Desenvolver os mecanismos informáticos que assegurem que os acessos realizados a dados pessoais de contribuintes por utilizadores internos são devidamente justificados e

fundamentados, tendo designadamente como referência o procedimento já adotado no desenho e concretização do sistema e-fatura;

d. Rever o quadro de contratação com entidades externas em matéria de procedimentos de acesso às bases de dados da AT, reforçando as regras e mecanismos de utilização das credenciais de acesso à informação fiscal por parte de utilizadores externos;
e. Criar mecanismos de certificação, monitorização e auditoria dos procedimentos de segurança informática, em particular aqueles relativos à proteção dos dados pessoais de todos os contribuintes; e
f. Estabelecer que o cumprimento do plano de ação deva ser objeto de auditorias regulares por parte da IGF, enquanto entidade externa à AT, especialmente no que diz respeito à segurança informática e à proteção do sigilo fiscal de todos os contribuintes, no quadro dos princípios da igualdade e da legalidade.

Foi ainda determinada a implementação, no mais breve prazo possível, de medidas consideradas urgentes e cautelares para assegurar uma efetiva proteção dos dados pessoais e tributários de todos os contribuintes, reequacionando, de imediato, o universo de utilizadores externos à AT com acesso a informação fiscal relevante.

Tendo como missão a preparação do plano de ação superiormente determinado e o acompanhamento da execução das medidas nele consagradas, bem como a identificação de novas medidas e a implementação de iniciativas concretas visando o reforço da efetiva proteção dos dados pessoais e tributários dos contribuintes, designadamente com o imediato reequacionamento do universo de utilizadores externos à AT, foi constituído por despacho da Senhora Diretora Geral da AT, de 2 de junho de 2015, um grupo de trabalho, constituído por representantes das áreas dos Sistemas de Informação, do Planeamento, dos Recursos Humanos e Formação, dos Recursos Financeiros, da Auditoria Interna, da Consultadoria Jurídica e Contencioso e do Gabinete da Diretora Geral.

II – PROTEÇÃO DE DADOS PESSOAIS E CONFIDENCIALIDADE FISCAL

O artigo 35.º da Constituição da República Portuguesa (CRP), sob a epígrafe "Utilização da Informática", vem consagrar o direito à proteção dos dados pessoais, de todo e qualquer cidadão, face ao uso da informática, remetendo para a lei a delimitação do conceito de dados pessoais.

No entanto, a regulamentação do citado preceito constitucional operou-se, inicialmente, com a Lei n.º 10/91, de 29 de abril, entretanto revogada com a entrada em vigor da Lei n.º 67/98, de 26 de outubro, Lei de proteção de dados pessoais (LPD), que procedeu à transposição para a ordem jurídica portuguesa da Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

O âmbito de aplicação da LPD circunscreve-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados.

Nos termos da LPD, no seu artigo 3.º, al. a) entende-se por dados pessoais: "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

No que se refere à definição de tratamento de dados pessoais a LPD, no seu artigo 3.º, al. b), dispõe que será considerado tratamento de dados pessoais "… («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição".

A referida Diretiva previa no seu artigo 8.º, um tratamento diferenciado para categorias específicas de dados e o legislador nacional proibiu no artigo 7.º da LPD o tratamento de dados sensíveis, considerando como tais o "tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos", contemplando contudo algumas exceções devidamente delimitadas no mesmo artigo.

O tratamento de dados pessoais deve ser feito observando o respeito por determinados princípios gerais, nomeadamente o princípio da transparência consubstanciado no direito à informação e no direito de acesso, garantidos ao titular dos dados, e o princípio da finalidade, que estabelece que os dados só

podem ser recolhidos para finalidades prévia e legitimamente determinadas e só podem ser tratados de forma compatível com essa finalidade.

O tratamento de dados pessoais deve também observar princípios relativos à qualidade dos dados, como é o caso do princípio da licitude e lealdade, do princípio da adequação, pertinência e proporcionalidade, do princípio da exatidão, atualização e tempo de conservação dos dados.

Na prossecução das suas atribuições a AT recolhe informação de diversa natureza e, nessa medida, estão abrangidos pelo sigilo fiscal todos os dados relativos aos contribuintes que respeitem, ainda que indiretamente, à respetiva capacidade contributiva e à situação tributária ou que tenham natureza pessoal nos termos da LPD.

O dever de confidencialidade determina que a AT não utilize os elementos revelados pelo contribuinte, para outros fins que não aqueles que lhe estão legalmente confiados, impondo que não possam ser revelados os dados que, no exercício das suas atribuições, recolha ou venha a recolher sobre a situação tributária dos contribuintes e os elementos de natureza pessoal que obtenha no procedimento.

O dever de confidencialidade surge como garantia de confiança entre os contribuintes e a Administração Tributária, assentando aquele, não só, mas também, na proteção dos dados pessoais.

O artigo 64.º da LGT ao convocar conceitos da legislação relativa à proteção de dados pessoais, sem lhes atribuir sentido específico, invocando o princípio da unicidade do ordenamento jurídico, manda observar, no tratamento de dados pessoais pela AT as normas e princípios relativos à proteção de dados pessoais, devendo a AT garantir que todo o tratamento de dados é efetuado com respeito pelos direitos, liberdades e garantias dos contribuintes.

III – SEGURANÇA DA INFORMAÇÃO NA AT

A segurança nos sistemas de informação da AT contra ataques externos e tentativas de intrusão, tem ao longo dos anos, revelado padrões de grande eficácia, o que tem garantido a integridade da informação e a salvaguarda da confidencialidade dos dados pessoais dos contribuintes.

Constata-se, no entanto, que existem fragilidades estruturais com reflexo na proteção do sigilo fiscal dos contribuintes, em resultado, designadamente, de uma deficiente gestão e atribuição de perfis de acesso aos utilizadores, internos e externos, e ao facto de não terem sido cumpridas regras contidas nos documentos de política de segurança produzidos e implementados internamente.

Urge, por isso, proceder a uma significativa revisão da política da segurança da informação da AT, adotar medidas concretas que visem o reforço da segurança informática, rever os critérios e o processo de gestão e atribuição de perfis aos utilizadores, bem como, simultaneamente, garantir a efetiva

sensibilização dos colaboradores da AT, para o rigoroso cumprimento das regras em matéria de sigilo fiscal e de proteção dos dados pessoais de todos os contribuintes, com salvaguarda do princípio da legalidade e da igualdade.

Nesse sentido e tendo em vista o estudo e implementação das medidas a adotar no seio da AT, foram desenvolvidos contactos com entidades nacionais com competências nas áreas da segurança informática, consultados meios académicos especializados neste domínio e analisadas e estudadas outras experiências e *standards* internacionais, designadamente através de uma visita à Agência Estatal de Administração Tributária de Espanha, igualmente subordinada ao dever de confidencialidade.

IV – PLANO DE AÇÃO

Com o presente plano de ação, que esquematicamente se apresenta em Anexo, pretende-se dar resposta às recomendações formuladas pela CNPD e pela IGF nos respetivos relatórios, sobre as quais assentaram as determinações constantes do despacho nº. 105/2015-XIX, de 26 de maio de 2015, do Senhor SEAF.

Este plano é suportado por um conjunto de trinta medidas que se encontram anexas, das quais doze de concretização até 31 de julho de 2015, nove de concretização até 31 de dezembro de 2015, sete de concretização até 31 de dezembro de 2016, uma de concretização até 31 de julho de 2017 e uma última de periodicidade anual externa à AT. De salientar que do total das medidas, vinte e duas terão início durante o ano de 2015.

A implementação das medidas insertas no presente plano de ação, requer a existência de dotação disponível nos orçamentos de 2015 e 2016 (1ºT), num valor que se estima como não inferior a 5 M€, podendo esta estimativa sofrer alterações em função do resultado dos estudos já iniciados, da complexidade que vier a ser assumida no desenvolvimento das medidas e das recomendações que vierem a ser emanadas na sequência das auditorias à própria execução do plano.

1. Medidas a implementar em 2015

1.1 Medidas a implementar até 31 de julho de 2015

a) **Rever os documentos de Politica de Segurança e atualização do Código de Conduta** (M04, M05 e M26)

   Os documentos de Politica de Segurança existentes compreendem a Politica de Segurança da Informação, a Politica de Classificação da Informação, a Politica de Gestão de Risco, a Politica de

Segmentação da Rede e a Politica de Boas Praticas de Desenvolvimento de Aplicações Seguras. Destes documentos, a revisão da Politica de Segurança da Informação da AT ficará concluída ainda no corrente mês, assim como a atualização do Código de Conduta.

A revisão/atualização destes dois documentos constitui fator de precedência relativamente a outras medidas, das quais se destaca:

- A formalização da tomada de conhecimento destes documentos por parte dos trabalhadores da AT;

- A continuidade e o reforço do plano de formação e sensibilização para os princípios de segurança, ética e privacidade.

b) Rever os perfis de acesso às aplicações atualmente atribuídos

- **Utilizadores Externos** (M01 e M20)

Procede-se à revisão e redução dos perfis atualmente atribuídos, tendo em vista adequá-los ao indispensável para a execução das atividades e serviços que justificam a condição de utilizador externo.

Tendo em vista a gestão, o controlo e a acreditação prévia de todos os utilizadores externos foi desenvolvido um novo módulo na aplicação de Gestão de Recursos Humanos, com entrada em produção ainda durante o corrente mês de junho.

Complementarmente, será implementada a ligação daquele módulo ao Sistema de Gestão de Utilizadores (SGU), a qual constituirá o suporte ao registo do utilizador externo e à sua desactivação, a partir do momento em que o mesmo deixe de exercer funções na AT.

- **Trabalhadores da AT** (M17)

Procede-se à revisão dos perfis atualmente atribuídos, tendo em vista adequá-los ao estritamente necessário para o exercício de funções. Posteriormente, serão implementadas outras ações (previstas na M18), através das quais se procederá à revisão da estrutura de perfis, tendo em atenção as necessidades funcionais e operativas dos trabalhadores, procedendo-se igualmente à evolução do Sistema de Gestão de Utilizadores (SGU).

c) Implementar mecanismo informático para registo prévio da fundamentação e contextualização do acesso por parte do utilizador (M12)

Assegura-se o reforço da garantia de preservação do sigilo fiscal e, nessa medida, a proteção dos dados pessoais, através da introdução da obrigatoriedade do registo da fundamentação prévia, por via de um mecanismo informático de utilização simples, de todos os acessos às aplicações. Deste

modo, fica evidenciado o contexto em que se realizam os acessos aos dados confiados à AT, sem que daí resultem perdas de eficiência com impacto no serviço prestado aos cidadãos.

d) Rever o processo de gestão de contas de utilizador (M02)

Procede-se à revisão do processo de gestão de contas de utilizadores internos, tendo em vista garantir a desativação imediata das autorizações existentes logo que se verifiquem eventos considerados relevantes, designadamente em caso de aposentação ou desempenho de funções fora da AT.

Aumenta-se, igualmente, a periodicidade de transmissão da informação da área de recursos humanos à área de segurança informática e sublinha-se a obrigatoriedade de imediata desativação, através do SGU, das permissões concedidas.

e) Criar Comité de Ética, Segurança e Controlo (M03)

Pretende-se consagrar na estrutura da AT um Comité vocacionado para as matérias de ética, segurança e controlo, onde se poderá solicitar a colaboração de entidades externas ou especialistas nos respetivos domínios de atuação.

f) Retomar a divulgação periódica das *newsletters* de segurança, ética e privacidade (M28)

Visa a melhoria da divulgação periódica e permanente das matérias relacionadas com a segurança, ética e privacidade juntos dos trabalhadores da AT.

g) Desenvolver competências avançadas em matéria de proteção de dados e de segurança da informação (M24 e M25)

Tendo em vista a aquisição de conhecimentos específicos no âmbito destas matérias, encontra-se concluída a frequência por parte de trabalhadores da AT do Curso Avançado de Proteção de Dados, lecionado pelo Instituto de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa, e agendada a frequência no Curso Geral de Segurança da Informação Classificada, ministrado pelo Gabinete de Nacional de Segurança.

1.2 <u>Medidas a implementar até 31 de dezembro de 2015</u>

a) Integrar o sistema de Gestão de Utilizadores com a base de dados de recursos humanos no tocante às movimentações de colaboradores externos (M21)

Pretende-se que a inibição de perfis de acesso de colaboradores externos seja feita de forma automatizada e imediata nas situações em que os mesmos cessem ou suspendam funções na AT

b) Rever as cláusulas de sigilo e confidencialidade presentes nos contratos de aquisição de serviços a celebrar (M09)

A referida medida apresenta como objetivo o reforço da obrigatoriedade de salvaguardar o sigilo por parte das empresas que prestam serviços à AT e respectivos trabalhadores, estabelecendo como requisito base a credenciação de segurança dos mesmos, nos termos definidos pelo Gabinete Nacional de Segurança.

c) Rever o Plano de Gestão de Risco de Corrupção e Infrações Conexas (M06)

O PGRCIC deverá, à semelhança do que já se verifica em matéria associada ao sigilo fiscal, contemplar os riscos relacionados com a segurança informática na ótica dos acessos a dados pessoais e fiscais dos contribuintes.

d) Rever os Protocolos estabelecidos com Entidades Terceiras no âmbito da troca de informação (M10)

Visa a reavaliação dos protocolos face às alterações introduzidas pela Política de Segurança de Informação da AT.

e) Rever os Protocolos com Autarquias e Contratos de Emprego Inserção (IEFP) (M11)

Tendo em vista o reforço das condições e cláusulas de sigilo fiscal, serão revistos os protocolos autárquicos, bem como os contratos de emprego e inserção.

f) Intensificar as ações de formação e sensibilização previstas no Plano de Formação para os princípios de segurança, privacidade e ética (M22)

No âmbito da revisão, aperfeiçoamento e comunicação de valores pelos quais se deve reger a atuação da AT, importa realçar que, durante o 1.º trimestre de 2015, cerca de 20% dos colaboradores da AT já frequentaram ações formativas de sensibilização no domínio dos princípios inerentes à ética profissional e à proteção dos dados pessoais dos contribuintes.

Assume-se como prioritária a revisão do plano de formação, atualizando os seus conteúdos e alargando as ações formativas à totalidade dos colaboradores.

O programa formativo do curso, sob a designação “Normas de Conduta e Política de Segurança da Informação”, destina-se a dirigentes, chefias e aos demais colaboradores.

g) **Desenvolver curso específico sobre sigilo fiscal e proteção dos dados destinados a colaboradores externos** (M29)

O referido curso destina-se a consciencializar os técnicos externos à organização relativamente às obrigações a que estão vinculados no exercício das suas funções.

h) **Definir o "Protocolo de Utilização de Recursos Informáticos"** (M08)

Visa criar um Protocolo de assinatura obrigatória por parte de todos os trabalhadores, após a realização do curso "Normas de Conduta e Política de Segurança da Informação", assim como das ações de sensibilização anuais, referidas na medida M23.

i) **Destacar na intranet à documentação relativa a segurança** (M27)

Visa dar maior visibilidade aos documentos e à informação associados à segurança informática disponibilizados na intranet, designadamente no que concerne à política de segurança e código de conduta dos trabalhadores da AT.

2. <u>Medidas a implementar até 31 de dezembro de 2016</u>

a) **Rever a estrutura geral de perfis e do sistema de Gestão de Utilizadores** (M18)

Para efeitos de implementação da referida medida, serão consideradas as necessidades funcionais e operativas dos trabalhadores no sentido de permitir que os perfis definidos sejam adequados ao exercício de funções, assim como o reforço dos pontos de controlo associados aos perfis aplicacionais.

b) **Definir e caracterizar um sistema que permita monitorizar à posteriori e contextualizar a utilização e o acesso às aplicações e bases de dados da AT (**M14)

O referido sistema deverá assentar na conjugação da implementação de medidas de segurança que permitam a auditoria e controlo à posterior, tendo subjacente a análise integrada da atividade exercida pelos diversos serviços da AT.

c) **Iniciar o processo de certificação ISO IEC 27001/2013** (M07)

A implementação da presente medida será acompanhada por entidade externa acreditada no âmbito da ISO IEC 27001/2013, quer ao nível informático, quer ao nível do desenho de processos de negócio e suporte que se encontram no âmbito da certificação.

d) Elencar critérios de utilização de acesso à informação de todos os contribuintes (M15)

Nos termos da recomendações da CNPD e da IGF, após consulta do Comité de Ética, Segurança e Controlo, elencar critérios de utilização de acesso à informação de todos os contribuintes que permitam aferir procedimentos indevidos, observando os princípios da igualdade e da legalidade.

e) Formalizar os processos de comunicação interna no âmbito da auditoria e investigação (M19)

A referida medida visa assegurar a formalização das comunicações de dados no âmbito dos processos de auditoria e investigação, nomeadamente através da utilização do Sistema de Gestão Documental.

f) Implementar mecanismos tecnológicos de controlo e monitorização de acessos a bases de dados (M13)

A referida medida permitirá o registo detalhado de todas as operações efetuadas sobre as bases de dados da AT.

g) Implementar ação de sensibilização anual para os princípios de segurança, privacidade e ética (M23)

As ações de sensibilização anuais serão desenvolvidas sobre a plataforma e-learning e visam a atualização permanente do conhecimento destas matérias por parte dos trabalhadores da AT.

3. <u>Medidas a implementar até 31 de julho de 2017</u>

Normalização dos Logs das aplicações (M16)

Todas as aplicações registam *logs* de todos os acessos. Pretende-se com esta medida normalizar a estrutura de conteúdo dos mesmos.

4. <u>Medida a implementar com periodicidade anual</u>

Audição e revisão anual da implementação das medidas definidas (M30)

O presente Plano de Ação deverá ser objeto de auditorias regulares por parte da Inspeção-Geral de Finanças (IGF), enquanto entidade externa à AT, com especial enfoque no que respeita à segurança informática e à proteção do sigilo fiscal de todos os contribuintes, de acordo com o quadro dos princípios da igualdade e legalidade, com a primeira auditoria a realizar-se, desejavelmente, no início de 2016.

ANEXOS

MEDIDAS CAUTELARES	
M01	Rever as atribuições de perfis de acesso a utilizadores externos
M02	Rever o processo de gestão de contas de utilizadores
MEDIDAS DE CARÁTER ESTRUTURAL	
M03	Criar Comité de Ética, Segurança e Controlo
M04	Rever os documentos de Politica de Segurança
M05	Atualizar o Código de Conduta
M06	Rever o Plano de Gestão de Riscos de Corrupção e Infrações Conexas
M07	Iniciar o processo de certificação ISO IEC 27001/2013
M08	Definir o “Protocolo de utilização de recursos informáticos”
M09	Rever as cláusulas de sigilo e confidencialidade presentes nos contratos de aquisição de serviços a celebrar
M10	Rever os Protocolos estabelecidos com Entidades Terceiras no âmbito de troca de informação
M11	Rever os Protocolos com autarquias e Contratos de Emprego e Inserção (IEFP)
MEDIDAS OPERATIVAS	
M12	Implementar mecanismo informático para registo prévio da fundamentação/contextualização do acesso por parte do utilizador
M13	Implementar mecanismos tecnológicos de controlo e monitorização de acessos a bases de dados
M14	Definir e caracterizar um sistema que permita monitorizar à posteriori e contextualizar a utilização e o acesso às aplicações e bases de dados da AT
M15	Elencar critérios de utilização de acesso à informação de todos os contribuintes
M16	Normalizar os logs de aplicações
M17	Rever os perfis atualmente atribuídos
M18	Rever a estrutura geral de perfis e o sistema de Gestão de Utilizadores
M19	Formalizar os processos de comunicação interna no âmbito da auditoria e investigação
M20	Adaptar as Bases de Dados de Recursos Humanos para contemplar as entradas e saídas de colaboradores externos
M21	Integrar o sistema de Gestão de Utilizadores com a base de dados de recursos humanos no tocante às movimentações de colaboradores externos
MEDIDAS DE CARÁTER FORMATIVO	
M22	Intensificar as ações de formação e sensibilização previstas no Plano de Formação para os princípios de segurança, privacidade e ética
M23	Implementar ação de sensibilização anual para os princípios de segurança, privacidade e ética
M24	Inscrever trabalhadores da AT no Curso Avançado de Proteção de Dados do Instituto de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa
M25	Inscrever trabalhadores da AT no Curso Geral de Segurança da Informação Classificada do Gabinete Nacional de Segurança
M26	Formalizar a tomada de conhecimento da Politica de Segurança e do Código de Conduta por parte dos trabalhadores da AT
M27	Destacar na intranet a documentação relativa a segurança
M28	Retomar a divulgação periódica das newsletters de segurança, ética e privacidade

M29	Desenvolver um curso específico sobre sigilo fiscal e proteção dos dados destinado a colaboradores externos
CONTROLO DE EXECUÇÃO DO PLANO	
M30	Auditar e rever anualmente o estado da implementação das medidas definidas, com a primeira auditoria a realizar-se, desejavelmente, no inicio de 2016.

	LNHAS PRIORITÁRIAS DE AÇÃO	MEDIDA	HORIZONTE TEMPORAL	CALENDARIZAÇÃO
a.	Proceder à revisão e reformulação profunda do Plano de Segurança informática da AT, com especial enfoque no reforço da proteção dos direitos dos contribuintes	M04 - Rever os documentos de Politica de Segurança	Imediata	07-2015
b.	Rever, aperfeiçoar e comunicar os princípios e valores pelos quais se deve reger a atuação da AT, estabelecendo os mecanismos que garantam o seu efetivo conhecimento e a vinculação por parte de todos os funcionários, principalmente em matéria de proteção	M05 - Atualizar o Código de Conduta	Imediata	06-2015
		M26 - Formalizar a tomada de conhecimento da Politica de Segurança e do Código de Conduta por parte dos trabalhadores da AT	Imediata	06-2015
		M24 - Inscrever trabalhadores da AT no Curso Avançado de Proteção de Dados do Instituto de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa	Imediata	06-2015
		M28 - Retomar a divulgação periódica das newsletters de segurança, ética e privacidade	Imediata	07-2015
		M25 - Inscrever trabalhadores da AT no Curso Geral de Segurança da Informação Classificada do Gabinete Nacional de Segurança	Imediata	06-2015
		M22 - Intensificar as ações de formação e sensibilização previstas no Plano de Formação para os princípios de segurança, privacidade e ética	Médio Prazo	a partir de 07-2015

		M29 - Desenvolver um curso específico sobre sigilo fiscal e proteção dos dados destinado a colaboradores externos	Médio Prazo	4º Trimestre 2015
		M08 - Definir o "Protocolo de utilização de recursos informáticos"	Médio Prazo	4º Trimestre 2015
		M27 - Destacar na intranet a documentação relativa a segurança	Médio Prazo	4º Trimestre 2015
		M23 - Implementar ação de sensibilização anual para os princípios de segurança, privacidade e ética	Médio Prazo	2º Trimestre 2016
c.	Desenvolver os mecanismos informáticos que assegurem que os acessos realizados a dados pessoais de contribuintes por utilizadores internos são devidamente justificados e fundamentados, tendo designadamente como referência o procedimento já adotado no desenho e concretização do sistema e-fatura	M12 - Implementar mecanismo informático para registo prévio da fundamentação/contextualização do acesso por parte do utilizador	Médio Prazo	07-2015
		M17 - Rever os perfis atualmente atribuídos	Médio Prazo	07-2015
		M06 - Rever o Plano de Gestão de Riscos de Corrupção e Infrações Conexas	Médio Prazo	4º Trimestre 2015
		M14 - Definir e caracterizar um sistema que permita monitorizar à posteriori e contextualizar a utilização e o acesso às aplicações e bases de dados da AT	Médio Prazo	2º Trimestre 2016
		M18 - Rever a estrutura geral de perfis e o sistema de Gestão de Utilizadores	Longo Prazo	4º Trimestre 2016

		M16 - Normalizar os logs de aplicações	Longo Prazo	1º Trimestre 2017
		M13 - Implementar mecanismos tecnológicos de controlo e monitorização de acessos a bases de dados	Médio Prazo	4º Trimestre 2016
d.	Rever o quadro de contratação com entidades externas em matéria de procedimentos de acesso às bases de dados da AT, reforçando as regras e mecanismos de utilização das credenciais de acesso à informação fiscal por parte de utilizadores externos	M10 - Rever os Protocolos estabelecidos com Entidades Terceiras no âmbito de troca de informação	Curto Prazo	3º Trimestre 2015
		M11 - Rever os Protocolos com autarquias e Contratos de Emprego e Inserção (IEFP)	Curto Prazo	4º Trimestre 2015
		M09 - Rever as cláusulas de sigilo e confidencialidade presentes nos contratos de aquisição de serviços a celebrar	Curto Prazo	4º Trimestre 2015
e.	Criar mecanismos de certificação, monitorização e auditoria dos procedimentos de segurança informática, em particular aqueles relativos à proteção de dados pessoais de todos os contribuintes	M03 - Criar Comité de Ética, Segurança e Controlo	Imediata	06-2015
		M02 - Rever o processo de gestão de contas de utilizadores	Imediata	06-2015
		M07 - Iniciar o processo de certificação ISO IEC 27001/2013	Médio Prazo	2º Trimestre 2016
		M15 –Elencar critérios de utilização de acesso à informação de todos os contribuintes	Médio Prazo	2º Trimestre 2016
		M19 - Formalizar os processos de comunicação interna no âmbito da auditoria e investigação	Médio Prazo	2º Trimestre 2016
f.	Estabelecer que o cumprimento deste Plano de Ação deve ser objeto de auditorias regulares por parte da IGF, enquanto entidade externa à AT, especialmente no que respeita à segurança informática e à proteção do sigilo fiscal de todos os contribuintes	M30 - Auditar e rever anualmente o estado da implementação das medidas definidas, com a primeira auditoria a realizar-se, desejavelmente, no inicio de 2016.		Anual

	Reequacionar de imediato o universo de utilizadores externos à AT com acesso a informação fiscal relevante	M20 - Adaptar as Bases de Dados de Recursos Humanos para contemplar as entradas e saídas de colaboradores externos	Imediata	07-2015
		M01 - Rever as atribuições de perfis de acesso a utilizadores externos	Imediata	06-2015
		M21 - Integrar o sistema de Gestão de Utilizadores com a base de dados de recursos humanos no tocante às movimentações de colaboradores externos	Curto Prazo	4º Trimestre 2015