Deloitte.

# Políticas de Segurança de Informação a cumprir por terceiros - Específico

## Deloitte Portugal

Versão: 6
Data da 1ª versão: 14-09-2017
Data da presente versão: 27-02-2024
Classificação: Pública
Referência: SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Específico.docx

## Público Alvo - Aviso

Este documento é destinado a todos os terceiros (empresas ou pessoas em nome individual) que prestem serviços à Deloitte Portugal, e que: acedem a informação confidencial e/ou dados pessoais e/ou estão integrados em equipas Deloitte e/ou têm acesso à nossa rede e/ou têm atribuídos PC's da Deloitte. Devem, por isso, tomar conhecimento e assegurar o cumprimento do seu conteúdo.

No caso de prestação de serviços relacionados com Sistemas de Informação deve ser ainda tomado conhecimento e implementar o conteúdo constante no documento "SGSI_Políticas de Segurança de Informação a cumprir por terceiros _Anexo_Sist. Inform".

## Controlo de Versões - Aviso

Este documento é um documento controlado que revoga todas as anteriores versões. Quaisquer cópias com versões anteriores ou com data anterior à data de publicação expressa na folha anterior não deverão ser consideradas como válidas.

## Propriedade - Aviso

O presente documento contém informação propriedade da Deloitte Central Services, S.A. (firma membro da Deloitte em Portugal). Cópia, distribuição ou disseminação não autorizada da informação aqui contida constitui uma violação das políticas da organização e de direitos de propriedade.

## Generalidades - Aviso

Quaisquer nomes de produtos aqui utilizados são somente para fins de identificação, e podem ser marcas registadas das respetivas organizações.

Após a conclusão da prestação do serviço o terceiro compromete-se a devolver e/ou destruir quaisquer cópias do presente documento (formato físico e/ou digital), incorrendo em responsabilidade pelo incumprimento deste procedimento.

# Índice

# 1 Política de Utilização Aceitável de Ativos

## 1.1 Introdução

Este documento define a Política de Utilização Aceitável de Ativos de tecnologias de informação e comunicação da Deloitte Portugal, bem como as responsabilidades dos colaboradores na sua utilização, de forma a garantir a confidencialidade, disponibilidade e integridade da informação da Deloitte Portugal e dos seus clientes, colaboradores, fornecedores, etc. (doravante informação Deloitte Portugal).

## 1.2 Monitorização e auditoria

A Deloitte Portugal reserva-se no direito de monitorizar e auditar, sem aviso prévio, de modo aleatório e sempre que tal seja justificável por razões legítimas de negócio, e de acordo com a legislação aplicável em vigor:

- A informação e o *software* instalado nos computadores portáteis e dispositivos portáteis de armazenamento;
- As atividades realizadas, pelos seus colaboradores, nos sistemas de informação de suporte ao negócio disponibilizados pela firma;
- As atividades realizadas na internet;
- A origem, destino, assunto de emails e nome de anexos enviados.

## 1.3 Utilização dos computadores portáteis

### 1. Instalação de *software*

De forma a assegurar a proteção da informação da Deloitte Portugal e dos seus clientes, os colaboradores não podem:

- Instalar jogos de computador;
- Instalar *software* que permita a partilha de arquivos na internet (*software* P2P);
- Instalar *software* pessoal, mesmo que licenciado pelo colaborador;
- Instalar *software* ilegal (sem licenciamento ou sem aprovação prévia);
- Instalar outro tipo de *software* nos computadores sem que exista uma razão legítima de negócio devidamente justificada pelo *Manager* do projeto e autorizada pelo Diretor de IT.

### 2. Proteção física dos equipamentos

Os colaboradores devem garantir que tomam todas as precauções necessárias para proteger os equipamentos da Deloitte Portugal em sua posse e a respetiva informação, independentemente da forma como esta seja guardada, evitando o acesso indevido por terceiros, nomeadamente:

- **Nas instalações da Deloitte Portugal/clientes/hotéis/locais públicos:**

- Os equipamentos devem estar supervisionados, seguros com o cadeado disponibilizado juntamento com o computador, ou guardados num cacifo ou cofre.

- Nas viaturas:
  - Os equipamentos com informação de clientes não devem ser deixados nas viaturas.

- Em aviões:
  - Os equipamentos com informação de clientes levados em viagem não podem ser despachados na bagagem de porão.

- Na residência
  - Os equipamentos com informação de clientes não devem ser deixados desprotegidos, devendo a utilização do equipamento ser restrita ao utilizador ao qual está atribuído. É proibida a utilização dos equipamentos da Deloitte Portugal por parte de familiares ou amigos do colaborador.

## 3. Política de ecrã limpo

Se um colaborador da Deloitte Portugal ou de uma entidade externa, estiver ausente do seu local de trabalho, deve manualmente ativar o bloqueio do ecrã do seu computador, que obrigará à reintrodução da *password* para entrar na sessão, embora o sistema assegure automaticamente o bloqueio do ecrã ao fim de 10 minutos de inatividade.

Sempre que um colaborador da Deloitte Portugal ou de uma entidade externa, estiver a aceder a informação confidencial de clientes (no escritório, residência ou em locais públicos), deve ter o cuidado de posicionar o ecrã do seu computador de forma a não permitir a sua leitura por terceiros. Os colaboradores que habitualmente usam o seu computador em aviões ou comboios devem utilizar filtros de proteção do ecrã.

## 4. Proteções de segurança lógica do computador portátil

Os colaboradores não podem remover, desabilitar ou alterar as configurações dos sistemas de segurança (ex. *firewall*, mecanismos de encriptação, deteção de vírus e *software* malicioso, instalação de *patches, etc*), sem que exista uma razão válida de negócio e aprovação expressa para o efeito pelo Manager do projeto e autorizada pelo Diretor de IT.

## 5. Salvaguarda da informação (Backups)

Se atribuído um PC Deloitte, os colaboradores devem assegurar a ligação frequente à rede Deloitte para realização regular do *backup* dos dados existentes no seu computador portátil, de forma a prevenir a perda de informação. Para tal, deverão utilizar o *software* de *backup* disponibilizado pela Deloitte Portugal e seguir as respetivas instruções.

Nas localizações onde a ferramenta não esteja disponível, os colaboradores devem contactar o *Service Desk* e solicitar instruções de como proceder de forma a garantir uma cópia de segurança dos seus dados.

Caso seja realizada uma cópia para um dispositivo externo amovível o mesmo deverá ser encriptado, e não pode ser transportado em conjunto com o computador.

## 1.4 Dispositivos portáteis de armazenamento

A utilização de dispositivos portáteis de armazenamento (ex.: Pens USB, Discos externos, SD Cards, etc.) para armazenar, transferir ou transportar informação da Deloitte Portugal só é permitida se os mesmos forem previamente encriptados utilizando a tecnologia disponibilizada pela firma, de acordo com os procedimentos existentes.

Sempre que seja necessário disponibilizar a *password* para acesso à informação encriptada de um dispositivo portátil de armazenamento, esta deve ser comunicada oralmente ou enviada por sms, sem mencionar o objetivo da mesma. Nestas situações o colaborador deve assegurar que o dispositivo apenas contém a informação necessária para o destinatário.

Os dispositivos portáteis de armazenamento devem ser guardados em locais protegidos, quando não estejam em utilização, e sempre que um colaborador pretenda destruir um dispositivo amovível deve ser entregue no IT (que seguirá os procedimentos adequados de destruição segura), e não deve ser colocado em contentores existentes nos pisos dos escritórios.

Em situações em que o cliente necessite de transferir informação a colaboradores da Deloitte Portugal através de dispositivos portáteis, o colaborador deve exigir ao cliente que o dispositivo esteja encriptado ou, em alternativa, que a informação seja gravada no dispositivo sob a forma de um zip com encriptação e *password*, devendo a password ser fornecida por outra via (oralmente ou por SMS) sem referência ao seu objetivo.

## 1.5 Dispositivos móveis (telemóveis, smartphones, tablets)

Só é permitido o *download* de informação da Deloitte Portugal para dispositivos móveis (*smartphones*, *tablets*), se os mesmos:

- Forem propriedade da Deloitte ou de colaboradores da Deloitte;
- Tiverem instalado o software de gestão de dispositivos móveis (Mobile Device Management) e de proteção (Mobile Threat Defense) indicado pela Firma;
- Estiverem encriptados, e;
- Estiverem protegidos com *password* ou pin de acordo com as regras da firma em vigor. O serviço de georreferenciação das APP, principalmente as relacionadas com redes sociais, deverá, sempre que possível, estar desabilitado.

## 1.6 Gestão de passwords

É da responsabilidade do utilizador garantir a confidencialidade da *password* da sua conta individual de acesso aos sistemas de informação da Deloitte Portugal, sendo proibido partilhar a mesma.

Desta forma, o dono da conta é o único responsável por todas as consequências que a utilização indevida da mesma possa ter.

Os utilizadores devem aplicar boas práticas de segurança na proteção da sua *password*:

- As *passwords* não devem ser divulgadas a outras pessoas, incluindo quaisquer colaboradores da Deloitte Portugal, incluindo os administradores de sistemas ou colaboradores do ServiceDesk;
- Sempre que haja necessidade de guardar alguma *password* deverá ser realizado num programa que garanta a proteção das mesmas com criptografia.

Para garantir uma adequada gestão das *password*s são estabelecidas as seguintes regras:

- Robustez, da *password* gerada pelo sistema ou pelos utilizadores:
    - Ter mais de 10 caracteres;

- Incluir caracteres de, pelo menos, três das seguintes quatro classes:
    - Maiúsculas (A, B, C);
    - Minúsculas (a, b, c);
    - Números (0, 1, 2);
    - Caracteres não-alfanuméricos (#, &, %, @, -, *).
- Não conter o primeiro ou último nome do utilizador, de um familiar, de uma pessoa famosa, datas de nascimento ou outra informação pessoal;
- Não conter qualquer outro nome ou palavras facilmente associadas ao utilizador;
- Não deve ser uma palavra de um dicionário ou outra que faça parte de um dialeto ou gíria de qualquer idioma, nem qualquer uma dessas palavras escrita ao contrário;
- As últimas vinte e quatro *passwords* não podem ser reutilizadas.

- É exigido ao utilizador a alteração da *password* inicial que lhe foi atribuída e enviada, após o primeiro login;
- Por defeito o período de validade da *password* é de 84 dias. Findo este período, a *password* expira e o utilizador terá de a alterar para continuar a ter acesso aos sistemas de informação.
- A *password* deve ser alterada sempre que hajam suspeitas de que a mesma possa ter sido comprometida;
- A *password* não deve ser visualizada no ecrã enquanto está a ser inserida;
- Só é possível alterar a password a cada 24 horas;
- *Passwords* usadas pelos utilizadores em contas para fins particulares (tais como e a título de exemplo: emails pessoais), não devem ser usadas nas contas de acesso aos sistemas de informação da Deloitte Portugal;
- As *passwords* não devem ser armazenadas em sistemas de registo automático (por exemplo, Lembrar/guardar *password* no *browser*) ou nos telemóveis;
- O número consecutivo de tentativas erradas de acesso aos sistemas com uma *password* é limitado a 5. O sistema deve recusar o acesso quando este limite é atingido, bloqueando a conta do utilizador por um período de 30 minutos.

## 1.7 Vírus e código malicioso

Todos os computadores com acesso à rede da Deloitte Portugal, deverão ter um *software* de Antivírus devidamente legalizado e atualizado. Esta regra aplica-se não só aos computadores atribuídos a colaboradores da Deloitte Portugal como também a computadores de terceiros que necessitem de ligar os seus dispositivos à rede.

Os colaboradores da Deloitte Portugal devem tomar todas as medidas razoáveis para garantir que não são responsáveis pela introdução de código malicioso (Vírus, *Malware*, etc.) nos sistemas de informação e comunicação da firma. Isto inclui, sem limitar, o dever de não abrir anexos de fontes desconhecidas e não efetuar *downloads* de *software* não autorizado.

## 1.8 Utilização do sistema de correio eletrónico corporativo (email)

A Deloitte Portugal disponibiliza acesso a uma conta de *email* a todos os seus colaboradores, para desempenho das suas atividades profissionais.

O envio ou receção de emails relacionados com atividades de negócio da Deloitte Portugal só pode ser efetuado por via da utilização de contas de *email* da própria firma. Não é permitida a utilização de *emails* pessoais do colaborador (gmail, Yahoo, etc.) para comunicações relacionadas com o negócio da firma, sem que exista uma razão válida de negócio e aprovação expressa do sócio responsável pelo cliente para o efeito. De igual forma, não devem ser efetuadas comunicações relacionadas com o negócio da firma para *emails* pessoais de clientes ou colaboradores dos nossos clientes, sem aprovação prévia e razões de negócio justificadas pelo Partner do projeto.

Cada endereço de *email* pessoal está associado a um colaborador que é responsável pelo mesmo. O proprietário pode delegar autoridades sobre a sua caixa do correio, mas mantém toda a responsabilidade pelas ações do delegado.

### 1. *Passwords* da conta de *email*

As *passwords* das contas de *email* pessoais não podem ser partilhadas. Sempre que for necessário dar acesso a outro colaborador à sua conta de *email* (por razões justificáveis de negócio, tais como às assistentes administrativas), tal deve ser feito através das funcionalidades de delegação de permissões do sistema de *email*.

### 2. Anexos ao *email*

Os utilizadores devem evitar o envio de mensagens com anexos superiores a 50MB e para muitos destinatários pois podem congestionar o serviço de correio eletrónico. Se for absolutamente necessário, os ficheiros devem ser comprimidos para reduzir a dimensão da mensagem de correio eletrónico.

### 3. Contas de email atribuídas a colaboradores externos

Colaboradores com vínculo temporário à Deloitte Portugal ou colaboradores externos que necessitem de conta de *email* para o desempenho das suas funções, deverão ter conhecimento e concordar explicitamente com as políticas da Deloitte Portugal, assinando um documento para o efeito. Estes colaboradores deverão estar conscientes, que todas as mensagens, geradas e tratadas pelos sistemas de correio eletrónico e no âmbito dos projetos onde estão envolvidos, são consideradas propriedade da Deloitte Portugal.

As contas de *email* atribuídas a colaboradores externos deverão ser utilizadas exclusivamente para as atividades profissionais desenvolvidas no âmbito dos serviços contratados.

## 1.9 Utilização da rede telefónica

A rede telefónica interna deve ser utilizada para uso empresarial, com uso pessoal razoável permitido.

Adicionalmente, a rede telefónica da firma não deve ser utilizada para:

- Fazer chamadas para números de telefone de valor acrescentado com acesso a conteúdos ofensivos dos bons costumes, moralmente censuráveis, discriminatórios ou pornográficos;
- Efetuar comunicações ofensivas ou difamatórias, que desacreditem ou embaracem, ou que constituam assédio moral ou discriminatório;
- Promover ou realizar qualquer negócio que não seja negócio da firma; e / ou
- Promover ou defender questões, causas, instituições de caridade ou organizações de qualquer tipo (incluindo ativismo político) a menos que autorizados pela Deloitte Portugal.

# 1.10 Utilização da internet

A Deloitte Portugal disponibiliza um acesso corporativo à Internet, para que os seus colaboradores possam executar as suas atividades profissionais diariamente. O acesso à internet pode ser adicionalmente usado com o objetivo de participar em ações de formação e desenvolvimento de novos *skills* e competências.

Só é permitido o seu uso para fins pessoais de uma forma razoável, desde que:

- Não se traduza em consumo de recursos da firma com impacto no negócio;
- Não interfira com a produtividade do colaborador;
- Não impeça ou tenha impacto nas atividades de negócio da firma;
- Não viole as políticas da firma ou quaisquer requisitos de confidencialidade, disponibilidade ou integridade estabelecidos.

Todos os colaboradores da Deloitte Portugal devem estar conscientes que o acesso à Internet é monitorizado de modo não permanente e não sistemático.

Os colaboradores da Deloitte Portugal não devem utilizar a internet corporativa da firma para:

- Atividades pessoais tais como:
    a. Ouvir e/ou fazer *download* de música;
    b. Ver vídeos e fazer *streaming*;
    c. Jogar ou aceder a *sites* de jogos ou apostas *online*;
    d. Organizar jogos ou administrar fóruns de jogos;
    e. Aceder a redes sociais, sem que seja com um propósito justificável e de negócio.

É expressamente proibido utilizar a internet corporativa da firma para:

- Fazer o *download* de *software* ilegal ou *software* não licenciado (quando o mesmo está sujeito a regras de licenciamento);
- Fazer o *download* de *freeware* sem que exista uma razão legítima de negócio devidamente aprovada;
- Fazer o *download* ou copiar material protegido por direitos de autor, registo de marca, patente ou segredo comercial sem autorização do proprietário de tais direitos;
- Disponibilizar a terceiros *software* que seja propriedade intelectual da Deloitte ou licenciada para a mesma;
- Aceder a conteúdos considerados ilegais, imorais, não éticos, pornográficos, ofensivos, fraudulentos, entre outros.

A área de Technology Solutions pode bloquear o acesso a algumas páginas da Internet para utilizadores, grupos de utilizadores ou todos os colaboradores da organização, de forma a dar cumprimento às políticas de segurança e utilização aceitável em vigor.

## 1. Ligação segura à internet

O tráfego de acesso à internet através da rede interna da Deloitte Portugal deverá ser filtrado e autorizado através das *firewall* corporativas existentes.

Sempre que um colaborador necessitar de aceder à internet, através do seu computador portátil, fora da rede da Deloitte Portugal, não pode alterar ou desabilitar as configurações da *firewall* do computador portátil.

O acesso à rede internet deverá ser realizado através de redes de confiança, devidamente identificadas e seguidas as boas práticas de segurança:

- Caso se trate de uma rede Wi-Fi, esta deverá usar um protocolo de encriptação, de preferência WPA-2;
- Não usar redes Wi-Fi publicas que não usem nenhum protocolo de segurança;
- Sempre que possível, deverão ser evitadas a utilização de quaisquer redes Wi-Fi publicas, de hotéis ou aeroportos;
- Sempre que possível, o acesso fora da Deloitte deverá ser realizado através do Hotspot do telefone.

## 1.11 Engenharia social

Os colaboradores da Deloitte Portugal não podem revelar informação confidencial de Clientes ou da firma, contactos ou outra informação de colaboradores a terceiros desconhecidos sem autorização prévia do CISO. Caso o colaborador tenha dúvidas sobre a autenticidade da chamada, *email* ou outra comunicação, deve procurar orientações e notificar o PT Security (ptsecurity@deloitte.pt).

Os colaboradores da Deloitte não devem fornecer o seu nome de utilizador através de qualquer *link* de *email*, telefonema ou outro método até que o solicitante esteja positivamente identificado e verificada a necessidade para obtenção dessa informação.

É proibido ao utilizador fornecer a sua *password* a terceiros dentro ou fora da firma. Caso seja solicitada esta informação através de uma chamada telefónica, *email* ou outra forma de comunicação o utilizador deve comunicar este evento de segurança ao PT Security (ptsecurity@deloitte.pt), assim que possível.

## 1.12 Serviços de Cloud

É proibido o envio de informação da firma ou de clientes para serviços de *Cloud,* seja para partilha de informação, infraestruturas ou outro tipo de serviços, sem que os respetivos fornecedores desses serviços e/ou as suas soluções aplicacionais estejam expressamente aprovados e autorizados pela Deloitte Portugal.

## 1.13 Transferência ou partilha de informação

A informação confidencial da Deloitte Portugal deve ser adequadamente protegida quando transferida entre colaboradores, clientes ou entidades externas autorizadas.

Desta forma, não é permitida:

- A utilização de programas ou serviços para partilha de informação que não sejam autorizados pela Deloitte;
- A partilha de informação, utilizando Pen USB ou discos externos, sem que os mesmos estejam encriptados;
- A transferência de ficheiros através de FTP (*File Transfer Protocol*);
- Outros serviços, dispositivos ou suportes sem que sejam devidamente autorizados pela Deloitte.

Os canais de transferência de informação confidencial de clientes em formato digital ou físico com terceiros autorizados devem assegurar, sempre que possível, a existência de mecanismos de controlo que protejam a informação contra interceção, cópia ou modificação não autorizada, alterações de percurso ou destruição acidental ou propositada.

Sempre que possível deverão ser utilizados mecanismos aprovados de cifra na transferência digital de informação confidencial de clientes e *software* de e para o exterior, independentemente do canal de comunicação utilizado e do terceiro autorizado.

Devem ser estabelecidos acordos para transferência de informação confidencial de clientes ou *software* com terceiros autorizados que abordem:

- As responsabilidades para o controlo e notificação da sua transmissão/expedição e entrega/receção;
- As responsabilidades e obrigações no caso de incidente de segurança da informação;
- As técnicas a utilizar para a identificação inequívoca por ambas as partes do nível de segurança dos conteúdos a transferir, procurando estabelecer pontos comuns de práticas a assegurar quando da sua transmissão e receção;
- As técnicas a utilizar para proteção de outros itens sensíveis a transferir, nomeadamente chaves de cifra;
- Os procedimentos a utilizar para o assegurar o rastreio de todas as fases do processo de transmissão e receção e o seu não-repúdio;

As regras de segurança mínimas para o seu empacotamento, caso aplicável, e transmissão.

## 1.14 Acesso de terceiros à rede da Deloitte

O acesso às redes locais da Deloitte Portugal deverá ser realizado preferencialmente por equipamento que seja propriedade da firma. No entanto, em casos excecionais e devidamente justificados, será permitida a ligação, por cabo, de equipamentos que sejam da propriedade de colaboradores externos ou de fornecedores de serviços, exclusivamente para desempenho das funções contratadas, depois de devidamente verificados e aprovados pela área de IT, de acordo com as políticas de controlo de acessos a sistemas (ver capítulo 22 do presente documento).

Aos clientes e visitantes é permitida a ligação à internet, através da rede *wireless* com identificação "GuestDNET", devendo ser solicitada a chave de acesso na receção da Deloitte Portugal.

## 1.15 Ligação de equipamentos da Deloitte à rede de terceiros

Os computadores disponibilizados pela Deloitte Portugal podem, com a aprovação prévia do LCSP e do cliente, conectarem-se à sua infraestrutura e recursos de IT do Cliente.

É permitida a instalação e configuração de *software*, para acessos remotos a redes de clientes, em computadores da Deloitte, quando devidamente autorizados pelo cliente e autorizados pela área de IT.

É permitida a configuração de VPN Site-to-Site entre redes das instalações da Deloitte e de clientes, quando devidamente autorizada e configurada pela área de IT da Deloitte e do Cliente. A rede da Deloitte deverá ser uma rede criada para o efeito e não a rede interna da Deloitte.

## 1.16 Controlo de acessos a sistemas

### 1. Colaboradores Externos (*long-term*)

Aos colaboradores externos da Deloitte Portugal (colaboradores em regime de trabalho temporário, subcontratados, fornecedores externos, etc.), só devem ser concedidos acessos à rede, sistemas e aplicações de suporte ao negócio, de acordo com a função que vão executar, ao abrigo do contrato com a Deloitte Portugal, e somente pelo período necessário.

O acesso de colaboradores externos deve requerer o estabelecimento de um acordo formal de confidencialidade.

Deverá existir um responsável na Deloitte Portugal pelo colaborador externo que terá como obrigação solicitar, justificar e aprovar:

- A atribuição de acessos ao colaborador externo e o período necessário;
- A alteração do período durante o qual o colaborador necessita dos acessos;
- A remoção atempada dos acessos assim que termine o período do contrato com o colaborador externo.

É permitida a ligação, por cabo, às redes locais dos edifícios da Deloitte Portugal, de equipamento que seja da propriedade dos colaboradores externos e exclusivamente para desempenho das suas funções, depois de devidamente verificados pela equipa de IT, de forma a garantir os requisitos mínimos para acesso à rede, nomeadamente:

- A versão mínima do Sistema Operativo deverá estar de acordo com a versão usada nos PC's da Deloitte Portugal ou superior;
- O Sistema Operativo deverá ter instaladas as últimas atualizações de segurança;
- Ter instalado um *software* de antivírus devidamente atualizado;
- Respeitar o processo de acesso à rede local em vigor.

## 2. Colaboradores Externos (intervenções esporádicas de suporte e manutenção)

Aos colaboradores externos da Deloitte Portugal, que se incluem na categoria de prestadores de serviços de IT que necessitam de fazer intervenções esporádicas para efeitos de manutenção periódica de sistemas ou apoio na resolução de problemas, só devem ser concedidos acessos à rede, sistemas e aplicações de suporte ao negócio, de acordo com a função que vão executar, ao abrigo do contrato com a Deloitte Portugal, e somente pelo período necessário.

O acesso de colaboradores externos deve requerer o estabelecimento de um acordo formal de confidencialidade.

Deverá existir um responsável na Deloitte Portugal pelo colaborador externo que terá como obrigação solicitar, justificar e aprovar:

- A atribuição de acessos ao colaborador externo e o período de tempo necessário;
- A alteração do período durante o qual o colaborador necessita dos acessos;
- A remoção atempada dos acessos assim que termine o período do contrato com o colaborador externo;
- Estabelecer o acordo de confidencialidade.

Adicionalmente, sempre que seja necessária a intervenção do fornecedor, devem ser garantidos os seguintes princípios:

- Acordar com o fornecedor a necessidade da intervenção a efetuar bem como o período da mesma;
- Reativar a conta do colaborador externo por esse período, sendo que finda a intervenção a mesma deve ser imediatamente desativada;
- Os trabalhos a serem efetuados pelo fornecedor devem ser acompanhados pelo colaborador do IT responsável pela intervenção.

É permitida a ligação, por cabo, às redes locais dos edifícios da Deloitte Portugal, de equipamento que seja da propriedade dos colaboradores externos e exclusivamente para desempenho das suas funções, depois de devidamente verificados pela equipa de IT, de forma a garantir os requisitos mínimos para acesso à rede, nomeadamente:

- A versão mínima do Sistema Operativo deverá estar de acordo com a versão usada nos PC da Deloitte Portugal ou superior;
- O Sistema Operativo deverá ter instaladas as últimas atualizações de segurança;
- Ter instalado um *software* de antivírus devidamente atualizado;
- Respeitar o processo de acesso à rede local em vigor.

## 1.17 Política de secretária limpa

Quando um colaborador da Deloitte Portugal ou de uma entidade externa, estiver ausente do seu posto de trabalho, todos os documentos em papel e todos os dispositivos amovíveis de armazenamento de dados que possuam informação confidencial de clientes, devem ser removidos da secretária e armazenados de forma segura de acordo com os procedimentos para manuseamento de ativos de informação.

Este procedimento deve ser seguido nas instalações da Deloitte Portugal e nas instalações de clientes onde se encontre a prestar serviços.

## 1.18 Política de proteção da informação impressa

Os colaboradores devem garantir que tomam todas as precauções necessárias com a informação impressa em sua posse, evitando o acesso indevido por terceiros, nomeadamente:

- Nas instalações da Deloitte/clientes/hotéis/locais públicos:
    - Os documentos impressos com informação de clientes devem ser guardados num cacifo ou cofre sempre que não estejam a ser utilizados ou supervisionados pelo colaborador que os tem á sua guarda;
    - Os documentos impressos e não utilizados, ou encontrados nas impressoras devem ser destruídos de forma segura, de acordo com o procedimento de manuseamento de ativos em vigor.
- Nas viaturas:
    - Os documentos impressos com informação de clientes não devem ser deixados nas viaturas.
- Em aviões:
    - Os documentos impressos com informação de clientes levados em viagem não podem ser despachados na bagagem de porão.
- Na residência
    - Os documentos impressos com informação de clientes não devem ser deixados desprotegidos, devendo a utilização do equipamento ser restrita ao utilizador ao qual está atribuído.

Os documentos que contêm informação confidencial de clientes, devem ser imediatamente removidos de impressoras, máquinas de fax e fotocopiadoras.

Para evitar a exposição de informação confidencial de clientes a pessoas não autorizadas encontra-se implementado um sistema de códigos pessoais, nas impressoras, para acesso a estes equipamentos.

A informação em papel deve ser destruída de forma segura, de acordo com o procedimento de manuseamento de ativos em vigor.

## 1.19 Direitos de autor

Nos termos do regime de obra por encomenda, todas as criações intelectuais relacionadas, direta ou indiretamente, com a atividade desenvolvida da Deloitte, nomeadamente invenções, ideias, estudos, desenvolvimentos e aperfeiçoamentos da autoria dos colaboradores da Deloitte Portugal, bem como os suportes em que as mesmas se materializam, são propriedade intelectual e exclusiva da Deloitte, sem que, por tal facto aos colaboradores seja reconhecido o direito a qualquer remuneração ou compensação adicional.

## 1.20 Devolução dos bens da firma

O colaborador tem como obrigação de entregar à Deloitte Portugal, e até à data da cessação do contrato/prestação de serviços:

- Qualquer bem (equipamentos físicos e licenças de *software*), que seja propriedade da Deloitte Portugal, e que lhe tenha sido cedido para o exercício das suas funções;
- Todos os materiais de trabalho, documentos, informações e dados em seu poder, qualquer que seja o suporte em que os mesmos se apresentem, relativos à Deloitte, aos clientes e fornecedores deste, ou que constituam propriedade intelectual ou *know-how* da Deloitte.

# 2 Política de Controlos Criptográficos

## 2.1 Política de controlos criptográficos

Toda e qualquer informação que seja partilhada via serviços web na rede interna da Deloitte deverá, sempre que possível, ser alvo de encriptação. Por exemplo: TLS, HTTPS ou SFTP.

Toda e qualquer informação que seja disponibilizada para o exterior (internet) a partir de sites internos da firma deverá ser alvo de encriptação.

É requerida a disponibilização de mecanismos que permitam a criação de tuneis de comunicação seguros para transmissão de informação entre dispositivos da Deloitte Portugal e a infraestrutura de rede interna da firma, quando acedidos a partir da rede Internet.

No caso particular da informação confidencial de clientes transmitida para o exterior através de correio eletrónico esta deve, sempre que possível, ser alvo de cifra recorrendo a mecanismos ou técnicas aprovadas e identificadas na Política de uso aceitável de ativos da firma.

As *passwords* de sistemas e de utilizadores quando transmitidas através da rede ou salvaguardadas em formato digital devem ser protegidas usando técnicas criptográficas, recomendando-se neste caso a utilização de algoritmos não reversíveis (hash).

Os dados transmitidos através de redes sem fio devem ser alvo de encriptação por mecanismos de cifra que implementem o algoritmo SHA-256.

Os acessos para gestão administrativa de sistemas devem recorrer sempre que possível ao protocolo SSH, com chaves de 1024 bits, no mínimo. Àqueles dispositivos que não permitam implementar SSH não são permitidos acessos remotos e a sua gestão deverá ser efetuada por via de gestão local.

A utilização de certificados digitais requer que a entidade certificadora emitente seja aprovada previamente pela Deloitte Portugal.

Se exigido por lei, regulamento ou contrato, os dados devem ser criptografados de acordo com esses requisitos específicos, após aprovação da Deloitte Portugal.

As chaves criptográficas e outra informação secreta (*passwords*) serão alvo de salvaguarda de acordo com o tipo de serviço em causa. Estes serviços e respetivas necessidades de salvaguarda desta informação serão alvo de formalização em informação documentada de suporte ao SGSI e de acesso reservado.

Deverão ser formalizados os procedimentos e métodos seguros considerados necessários para a gestão do ciclo de vida das chaves criptográficas no contexto de produção. Das fases do ciclo a avaliar a pertinência de formalização contam-se:

- Geração de chaves para diferentes sistemas de cifra e aplicações;
- Emissão e obtenção de certificados digitais de chave pública;
- Distribuição de chaves;
- Salvaguarda de chaves;
- Alteração ou atualização de chaves;
- Revogação de chaves;
- Recuperação de chaves, perdidas ou corrompidas;
- Salvaguarda e arquivo de chaves;
- Destruição de chaves.

## 2.2 Glossário

- SFTP – Secure File Transfer Protocol
- SHA – Secure Hash Algorithm
- SMIME – Secure /Multipurpose Internet Mail Extensions (secure email)
- SSH – Secure Shell
- TLS - Transport Layer Security

# 3 Procedimentos para o Manuseamento de Ativos de Informação

## 3.1 Salvaguarda de informação confidencial de clientes

### 1. Informação em formato digital

Toda a informação confidencial de clientes deve ser alvo de salvaguarda nos repositórios centrais da Deloitte Portugal. A existência de informação confidencial de clientes fora dos repositórios centrais da Deloitte Portugal, nomeadamente nos *laptops*, *desktops* ou outros dispositivos móveis, deve ser restrita ao absolutamente necessário e pelo tempo mínimo possível. É responsabilidade do utilizador assegurar a cópia ou movimentação dessa informação dos dispositivos sob sua responsabilidade para os repositórios centrais da firma. Só após essa cópia ou movimentação da informação, é que o utilizador poderá proceder à eliminação da mesma nos seus dispositivos.

Não é permitida a salvaguarda de informação confidencial de clientes em sistemas externos não autorizados pela Deloitte Portugal.

No âmbito da prestação de serviços da firma, a salvaguarda de informação de suporte ao *engagement* poderá ocorrer noutros equipamentos e sistemas que o Cliente expressamente autorize por escrito, sendo para tal necessária a aprovação prévia do *partner* responsável pelo *engagement*.

### 2. Informação em formato físico

Toda a informação confidencial de clientes deve ser sempre alvo de salvaguarda em locais adequados que mitiguem o risco de acesso por terceiros não autorizados. Quando nas instalações de Clientes no âmbito da prestação de serviços da firma, o mesmo princípio deverá ser aplicado solicitando-se expressamente a disponibilização das medidas adequadas ao Cliente.

Sempre que não em utilização, a informação confidencial de clientes deve ser alvo de salvaguarda em locais ou compartimentos que possuam controlo de acesso ([1]).

Toda a informação confidencial de clientes em formato físico deve ser transposta, sempre que possível, para formato digital, utilizando-se para o efeito os serviços internos de "Digitalization" disponibilizados pelo departamento Office Administration. Após digitalização da informação deve o seu responsável avaliar a pertinência e possibilidade ([2]) da sua eliminação segura.

## 3.2 Utilização e processamento de informação confidencial de clientes

### 1. Informação em formato digital

Só é permitida a utilização e processamento de informação confidencial de clientes em aplicações, equipamentos e sistemas propriedade da Deloitte Portugal ou outros expressamente pré-aprovados pela firma ou pelo Cliente.

A impressão de informação confidencial de clientes deve ser restringida ao absolutamente essencial. Devem ser tomados cuidados especiais quando da impressão desta informação, nomeadamente:

- Estar presente junto ao equipamento de impressão enquanto esta está a ser impressa;
- Eliminar de forma segura quaisquer páginas que não estejam conformes ao resultado desejado e necessitem de reimpressão;
- No final da impressão assegurar-se que recolhe todas as folhas impressas.

[1] Exemplos: Arquivo do piso, cacifo individual ou de projeto, sala com chave em instalações de Cliente.

[2] Atenção: Por motivos de índole legal (valor probatório), poderá existir a necessidade de manutenção do documento original.

### 2. Informação em formato físico

Só é permitida a utilização e processamento de informação confidencial de clientes nas instalações da Deloitte Portugal, ou noutras previstas para efeitos de prestação de serviços a clientes.

## 3.3 Transporte e Partilha de informação confidencial de clientes

### 1. Informação em formato digital

Não é permitida a partilha de informação confidencial de clientes por recurso a sistemas externos ([3]) não autorizados pela Deloitte, devendo ser seguidas as orientações previstas no capítulo 1.13 -Transferência ou partilha de informação.

### 2. Informação em formato físico

Quando nas instalações da firma, a partilha de informação confidencial de clientes entre colaboradores ou com terceiros autorizados requer entrega da mesma em mão.

O envio e transporte de informação confidencial de clientes para entidades externas por recurso a serviços postais ou de estafeta requer que esta informação, no mínimo:

- Seja colocada em sobrescrito Deloitte, inscrevendo-se na sua face o endereço completo do destinatário, o nome do destinatário final e a palavra “Confidencial”;
- De seguida, se coloque este sobrescrito no interior de um outro sobrescrito, não identificado, inscrevendo-se na sua face o endereço completo do destinatário, o nome do destinatário final e apondo-se estampilha postal ou outros elementos necessários à execução do transporte, se necessário;
- Seja enviada por recurso a serviço externo de correio postal, estafetas ou colaboradores internos devidamente autorizados.

Que a informação esteja permanentemente sob supervisão ou proteção do colaborador.

### 3. Informação em formato verbal

É proibida a partilha verbal de informação confidencial de clientes a familiares, amigos, ou com outros colaboradores não diretamente relacionados com o tema em questão.

A partilha verbal de informação confidencial de clientes não deve ser efetuada em espaços públicos (exemplo: elevadores, transportes, restaurantes, etc.).

## 3.4 Eliminação de informação confidencial de clientes

### 1. Informação em formato digital

As cópias de informação confidencial de clientes devem ser alvo de eliminação de acordo com as seguintes regras:

- Equipamentos ou dispositivos móveis em utilização - eliminadas pelo utilizador, quando não sejam mais necessárias; é

[3] Exemplos: Servidores FTP, Dropbox, Wetransfer, GoogleDrive, iCloud.

responsabilidade do utilizador assegurar a cópia ou movimentação dessa informação dos dispositivos sob sua responsabilidade para os repositórios centrais da firma antes da sua eliminação;

- Equipamentos para reutilização ou abate - são alvo de eliminação/destruição de acordo com procedimentos pré-estabelecidos a executar pelo IT.

## 2. Informação em formato físico

Cópias de informação confidencial de clientes em formato físico, quando deixarem de ser necessárias devem ser inutilizadas com recurso a uma trituradora ([4]) ou colocadas nos contentores para destruição de papel.

[4] capacidade mínima de corte cruzado ou nível de segurança P-3 - DIN 66399 = ≤2 mm de largura e qualquer comprimento ou partículas ≤320 mm² (de qualquer largura)

Deloitte.