Deloitte.

Políticas de Segurança de Informação a cumprir por terceiros - Geral

Deloitte Portugal

Versão: 4
Data da 1ª versão: 14-09-2017
Data da presente versão: 12-08-2021
Classificação: Restrita
Referência: SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Geral.docx

Público Alvo - Aviso

Este documento é destinado a todos os terceiros (empresas ou pessoas em nome individual) que prestem serviços à Deloitte Portugal, devendo tomar conhecimento e assegurar o cumprimento do seu conteúdo.

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 Segurança de Informação

1.1 Política de Segurança de Informação

A proteção no tratamento, salvaguarda e transmissão de informação confidencial de clientes de forma consistente com os requisitos profissionais, éticos, legais, regulamentares e contratuais, é uma das maiores prioridades da Deloitte Portugal e algo que é considerado fundamental para o sucesso da firma. A perda ou roubo de informação confidencial pode ter consequências graves a nível legal, financeiro e/ou reputacional, estando a Deloitte Portugal comprometida com a salvaguarda da confidencialidade, integridade e disponibilidade da informação confidencial de clientes e da própria Deloitte quer esta se encontre em suporte físico, digital ou intelectual.

Desta forma, são princípios da política de segurança da informação garantir que:

- A informação está protegida contra acessos não autorizados;
- A confidencialidade da informação está garantida;
- A integridade da informação é mantida;
- Todas as leis e regulamentos aplicáveis são respeitados;
- Os planos de continuidade de negócio apropriados são mantidos e testados regularmente; e
- Todas as quebras de segurança da informação detetadas ou sob suspeita, são investigadas pelas áreas com competência para o efeito.

Para tal a Deloitte Portugal mantém um Sistema de Gestão de Segurança de Informação (SGSI) constituído por políticas, processos e procedimentos e que foi desenhado para manter, rever e continuamente melhorar a segurança de informação na Deloitte Portugal, tendo por base uma avaliação do risco existente. O SGSI visa:

- Garantir que todos os colaboradores têm conhecimento e cumprem esta Política, e outras políticas e/ou procedimentos de segurança existentes;
- Definir e comunicar responsabilidades ao nível da Segurança de Informação na firma;
- Promover a consciencialização contínua sobre a segurança de informação e realizar programas de formação para garantir que todos os colaboradores compreendem a forma como a segurança de informação faz parte das suas funções e as responsabilidades que têm na proteção da confidencialidade, integridade e disponibilidade da informação;
- Incluir a segurança de informação como componente essencial de todos os aspetos de planeamento e operações de negócio;
- Avaliar continuamente as ameaças de segurança de informação, garantindo que estas são identificadas e geridas tendo por base a avaliação de risco e com a aplicação dos controlos adequados;
- Promover a proteção adequada da infraestrutura de sistemas de informação e comunicações da firma contra perda, má utilização ou acessos indevidos;
- Promover a deteção, registo, reporte e investigação de incidentes de segurança de forma eficaz e eficiente para garantir a minimização dos impactos deste tipo de incidentes na firma;
- Garantir a implementação e teste, dos planos de continuidade de negócio que assegurem a continuidade das operações, minimizando o impacto da ocorrência de um incidente de segurança ou de uma situação de emergência;
- Garantir a disponibilização dos recursos necessários a garantir a efetiva manutenção e melhoria contínua do SGSI; e
- Promover a revisão contínua dos mecanismos e processos de segurança para assegurar que são efetivos, relevantes e adequados às necessidades da firma.

1.2 Responsabilidades

Todos os colaboradores, bem como terceiros que, de alguma forma, possam interagir com informação confidencial de clientes da Deloitte Portugal, estão obrigados a cumprir e a fazer cumprir todas as políticas de segurança da informação da firma, devendo prontamente reportar ao CISO qualquer incidente de segurança, ou seja, qualquer evento que possa provocar, ou que tenha provocado, uma quebra de segurança da informação.

2 Política de Segurança Física e Ambiental

Poderão ser emitidos cartões de identificação especiais [1] a terceiros que necessitem de acesso temporário às instalações da Deloitte Portugal. Estes serão considerados terceiros pré-credenciados. Este acesso deve ser configurado para apenas permitir o acesso às áreas a que os terceiros pré-credenciados necessitam de aceder para o exercício das funções para as quais foram autorizados ou contratados. A disponibilização destes cartões deverá ser alvo de pré-autorização, emanada pelo colaborador da firma responsável pela presença do terceiro, especificando as áreas a que necessitará de aceder. Deve ser sempre requerida a utilização do cartão de identificação disponibilizado de forma claramente visível durante a permanência nas instalações da firma.

Para cada edifício da Deloitte Portugal devem ser identificados os seguintes perímetros de segurança física:

- Perímetro exterior – áreas públicas; todas as áreas que antecedem o perímetro semipúblico;
- Perímetro semipúblico – áreas de acesso controlado [2] nas quais podem circular e permanecer elementos externos à Deloitte Portugal;
- Perímetro reservado – áreas de trabalho dos colaboradores da Deloitte Portugal;
- Perímetro seguro ou área segura – áreas onde resida, se salvaguarde ou se processe informação confidencial de clientes ou onde existam ativos produtivos de suporte à infraestrutura de informação e comunicação da firma.

Os perímetros semipúblicos devem respeitar as seguintes regras:

- Todos os terceiros sem credenciais de acesso que pretendam aceder a instalações da Deloitte Portugal só o poderão fazer após obtenção de autorização do visitado. Deve ser efetuado pelo pessoal da receção o registo do nome do terceiro antes da sua entrada nos escritórios da Deloitte Portugal;
- O acesso a estes perímetros por parte de terceiros sem credenciais deve ser acompanhado por um colaborador da receção, não necessitando de acompanhamento permanente enquanto se encontram nestes perímetros;
- O acesso a estes perímetros por parte de colaboradores da Deloitte Portugal e visitantes pré-credenciados deve ser efetuado mediante utilização do cartão de identificação da firma em sistemas de controlo de acessos eletrónicos.

Os perímetros reservados devem respeitar as seguintes regras:

- O acesso a este perímetro por parte de colaboradores da Deloitte Portugal ou terceiros pré-credenciados deve ser efetuado mediante utilização do cartão da firma em sistemas de controlo de acessos eletrónicos;
- O acesso fora do horário normal de trabalho deve ser sempre protegido por mecanismos de controlo de acessos com dois fatores de autenticação: cartão e PIN;
- Terceiros não credenciados só poderão entrar e permanecer neste perímetro quando acompanhados por um colaborador da firma;
- O acesso a este perímetro tem de ser alvo de gravação de imagens.

Os perímetros seguros ou áreas seguras devem respeitar as seguintes regras:

- Devem ser sempre protegidas por mecanismos de controlos de acessos com dois fatores de autenticação: cartão e PIN;
- Os colaboradores da Deloitte Portugal com acesso a áreas seguras devem ser alvo de autorização específica emanada pelo responsável da área em causa sempre que for uma exceção à matriz de acessos físicos aprovada. Estes devem constar de uma lista interna de concessões de acesso a áreas seguras que será mantida atualizada pelo mesmo responsável. Deverá ser efetuada, no mínimo, uma revisão anual dos elementos que integram esta lista;
- Quaisquer terceiros que necessitem de acesso a áreas seguras (DataCenters e Arquivos Centrais e Intermédios) devem ser alvo de autorização específica emanada pelo responsável da área em causa, registando-se qual a necessidade de acesso, o horário e alocação de tempo pré-autorizado bem como quaisquer outras informações consideradas pertinentes para o acesso em causa;

[1] Colaborador Externo ou Visitante Regular.

[2] Zonas após a área de receção de Clientes, fornecedores ou visitantes incluindo as salas de reuniões de clientes no piso 1 do Deloitte Hub.

- O acesso e permanência de terceiros em áreas seguras (DataCenters e Arquivos Centrais e Intermédios) deve ser alvo de acompanhamento permanente por colaboradores autorizados da firma;
- O acesso exterior aos DataCenters, Arquivos Centrais e Arquivos Intermédios deve ser alvo de gravação de imagens. No caso dos DataCenters, sempre que possível, deve ser colocada uma câmara de vigilância no interior do perímetro a fim de permitir a monitorização remota da presença de elementos no seu interior;
- Quando no desempenho de atividades em áreas seguras é proibido:
    - Fumar, comer ou beber;
    - Fotografar ou filmar, exceto quando previamente autorizado pelo responsável da área.
- Os equipamentos residentes em áreas seguras não devem ser retirados das instalações sem autorização prévia do responsável da área em causa e do responsável pelo ativo em questão;
- Qualquer equipamento ou informação em formato físico (para Arquivos Centrais e Intermédios) retirado(a) de uma área segura deve ser alvo de registo apropriado no qual será identificado: Data/Hora de movimentação, nome do colaborador responsável pela movimentação, motivo. Deve ser realizada a atualização do correspondente inventário de ativos de suporte do SGSI no caso de equipamentos de tecnologias de informação ou comunicação;
- Todos os ativos de suporte às infraestruturas de informação e comunicação a serem retirados destes perímetros devem ser previamente verificados quanto à necessidade de eliminação de qualquer informação confidencial de clientes e software licenciado;
- Sempre que possível o desempenho de atividades nas áreas seguras deve ser efetuado por mais do que um elemento a fim de se assegurar respostas adequadas em caso de incidente sobre um dos elementos e para prevenir atividades maliciosas;
- É proibida a existência de material não diretamente relacionado com as atividades de gestão e manutenção de infraestruturas tecnologias de informação e comunicação, exceto quando previamente autorizado pelo responsável da área. Esta permanência deve ser autorizada pelo mínimo de tempo considerado necessário;
- As áreas seguras devem ter sinalética adequada, no seu interior, a divulgar as proibições e recomendações em vigor;
- As áreas seguras não deverão ser identificadas como tal no seu exterior, exceto quando exigido por Autoridades competentes.

3 Política de Utilização Aceitável de Ativos

3.1 Divulgação de informação da Deloitte e exposição na Internet

Os colaboradores não podem:

- Publicar informação confidencial ou pública da Deloitte em *sites* externos, sem aprovação prévia e expressa da firma;
- Fazer comentários ou afirmações sobre a Deloitte Portugal em *newsgroups, instant messaging*, chat *rooms*, redes sociais ou outros fóruns públicos;
- Fazer comentários ou afirmações sobre os clientes e *engagements* em *newsgroups, instant messaging, chat rooms*, redes sociais ou outros fóruns públicos;
- Usar o endereço de *email* da Deloitte em comunicações públicas, *newsgroups, instant messaging, chat rooms*, redes sociais ou outros fóruns públicos, salvo se a participação nessas comunicações seja um requisito explícito da sua função na Deloitte e apenas com aprovação prévia;
- Publicar ou disponibilizar o endereço de *email* da Deloitte em websites, como email de contacto para receber comunicações;
- Participar em qualquer comunicação que seja ilegal ou que viole qualquer política da firma, incluindo (mas não limitado a) comunicações difamatórias, obscenas, racistas, sexistas ou que evidenciem preconceitos religiosos;
- Criar *web sites* ou páginas na internet que representem ou apresentem ofertas de produtos e serviços da Deloitte sem aprovação do departamento de marketing;
- Promover produtos, gerir negócios ou transações comerciais que não estejam diretamente relacionados com a sua função na firma;

Promover ou advogar causas, instituições de caridade ou instituições de qualquer tipo (incluindo ativismo político) a menos que seja expressamente autorizado pela firma.

3.2 Redes Sociais

Os colaboradores da Deloitte Portugal não podem utilizar a imagem ou o *Brand* da Deloitte, revelar informação confidencial de Clientes ou da firma, contactos ou outras informações de colaboradores, *engagements* ou clientes nas redes sociais.

3.3 Controlo de acessos físicos

1. Segurança dos edifícios

Nos termos da Política de Segurança Física e Ambiental:

- a entrada nos edifícios da Deloitte é controlada por cartões de acesso que são atribuídos a todos os profissionais, colaboradores externos e visitantes regulares (incluindo fornecedores de bens ou serviços com necessidade de ter acesso às instalações com carácter de regularidade) da Deloitte;
- os visitantes pontuais (clientes ou terceiros que venham ter reuniões no escritório) devem dirigir-se à receção para registo e posterior acompanhamento;

- todas as entradas e saídas de edifícios da Deloitte são monitorizadas por camaras de circuito interno, ficando as imagens guardadas por um período de 30 dias;
- a gestão das camaras de CCTV é da responsabilidade da área de Office Administration - Facilities da Deloitte.

2. Regras globais para os colaboradores

Os cartões para além de permitirem o acesso aos edifícios e respetivas zonas de segurança, de acordo com as funções de cada colaborador, identificam a pessoa como sendo colaborador da Deloitte, sendo obrigatório exibi-lo em local visível, preferencialmente usando a fita oficial para colocação do cartão ao pescoço.

Este cartão é da responsabilidade do colaborador e deverá ser usado exclusivamente pelo mesmo, sendo proibido o empréstimo a outros colaboradores ou a terceiros.

Qualquer colaborador da Deloitte deverá estar atento e abordar qualquer pessoa que não tenha visível o cartão identificador, reportando possíveis falhas de segurança de acordo com o processo de gestão de incidentes de segurança.

Em caso de perda, avaria ou esquecimento do cartão, o Profissional, Colaborador Externo ou Visitante Regular deve dirigir-se à receção.

3. Regras globais para visitantes

Os visitantes, incluindo os funcionários de entidades externas e que prestam serviços de manutenção regular de equipamentos, devem seguir os procedimentos em vigor relativos ao acesso às instalações da Deloitte Portugal.

Deloitte.