Deloitte.

Políticas de Segurança de Informação a cumprir por terceiros – Anexo: Sistemas de Informação

Deloitte Portugal

Versão: 2
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__Anexo_Sist._Inform.docx

Público Alvo - Aviso

Este documento, complementa os documentos "SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Geral" e "SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Específico", e é destinado a todos os terceiros (empresas ou pessoas em nome individual) que prestem serviços relacionados com Sistemas de Informação 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 Requisitos de Segurança para Novos Sistemas de Informação

1.1 Considerações sobre especificação e análise de requisitos de segurança da informação

Sempre que se inicie um processo de desenvolvimento de um novo sistema de informação devem ser identificados, documentados e revistos regularmente os requisitos de segurança da informação utilizando diversos métodos, nomeadamente: derivar requisitos de conformidade face a políticas e regulamentação, modelação de ameaças ou revisões de incidentes de segurança da informação.

A identificação e a gestão dos requisitos de segurança da informação e processos associados deve ser integrada nos estágios iniciais deste tipo de projetos.

Os requisitos de segurança da informação para novos sistemas de informação devem considerar os seguintes vetores de análise:

- *Hosting* e segregação de ambientes:

  Qualquer sistema ou aplicação da Deloitte Portugal deve ficar alojado num *host* aprovado pela firma, quer se trate de um *data center on premises*, *cloud hosting*, *SaaS (software-as-a-service)* ou qualquer outro modelo a contratar; o ambiente produtivo deve ser segregado dos ambientes não produtivos, com requisitos de segurança específicos, nomeadamente regras de autenticação e de autorização.

- Autenticação:

  Prevenção do acesso aos sistemas, aplicações e seus dados por parte de utilizadores desconhecidos ou não autorizados; deve existir o máximo nível de confiança quanto à identidade dos utilizadores (por ex: *userid* e *password*, autenticação por dois fatores, SSO, etc.), cumprindo com as normas e standards em vigor na firma, tal como a obrigatoriedade de utilização do MFA (*Multi Factor Authentication)* para o caso das aplicações acessíveis através da internet.

- Autorização:

  Deve ser aplicado o princípio do menor privilégio: cada utilizador devidamente autenticado só deverá ter acesso aos dados de que necessita para a execução das suas funções; devem existir processos diferenciados de autorização e aprovisionamento para utilizadores comuns, utilizadores privilegiados e de serviço.

- Papéis, responsabilidades e segregação de funções:

  Deve ser endereçado o potencial risco de abuso de privilégios de acesso à informação; os acessos e papeis de cada sistema ou aplicação devem ser assignados aos utilizadores com base na real necessidade de informação para a realização das respetivas atividades e tendo em conta a segregação de funções: deve ser assegurado que a execução de atividades críticas para o negócio e o respetivo controlo não são realizados pelo mesmo utilizador.

- Privacidade e confidencialidade:

  Devem ser definidos os níveis de proteção e controlos apropriados, por forma a salvaguardar a disponibilização e divulgação indevidas de informação confidencial ou sensível.

- Integridade:

  Devem ser definidos os níveis de proteção e controlos apropriados, por forma a salvaguardar a modificação indevida de dados ou transações; as aplicações *cloud* e *mobile* devem prever mecanismos específicos de proteção, pela maior exposição ao risco de ciberataques que provoquem não integridade dos dados.

- Disponibilidade

  Devem ser incluídos na arquitetura do sistema ou aplicação os requisitos de negócio quanto à sua disponibilidade (ex: carga, *downtime*, redundância, disponibilidade contínua, etc.).

- *Logs* de auditoria e monitorização:

  Deve ser definido o rastreamento das atividades dos utilizadores realizadas nos sistemas e aplicações, com especial atenção às ações críticas para o negócio; para cada tipo de ação no sistema ou aplicação, deve ser definido o nível de detalhe de informação a ser gerada e o seu local de salvaguarda, incluindo as ações realizadas pelos utilizadores com acessos privilegiados. Os *logs* devem ser monitorizados de forma sistemática e com frequência, por forma a que seja possível a obtenção de alertas de atividades anómalas ou suspeitas e proceder à análise forense dessas atividades.

- Fuga de informação:

  Estabelecimento de controlos de segurança que previnam a fuga de informação sensível e confidencial; os sistemas e aplicações devem ser monitorizados com frequência, por forma a que sejam detetados acessos atípicos à informação (ex: excesso de *queries*, *reports* ou *downloads* face ao padrão normal de utilização). Deve ter-se especial atenção ao desenho e arquitetura de aplicações *mobile*, por forma a que sejam incorporados mecanismos de proteção contra ciberataques, nomeadamente de *reverse engineering*.

- Plano de continuidade de negócio e recuperação de desastres:

  Os *owners* funcionais dos processos abrangidos pelo sistema ou aplicação em causa, devem rever o Plano de Continuidade de Negócio da Deloitte Portugal e garantir que foram incluídos os requisitos de recuperação em caso de desastre, nomeadamente o RTO (Recovery Time Objective) e o RPO (Recovery Point Objective); a arquitetura do sistema ou aplicação deve incluir esses requisitos, nomeadamente ao nível de *hosting*.

- Outras considerações gerais:

  Antes de se iniciar a fase de desenho do sistema ou aplicação, deve garantir-se que os vários processos de segurança foram validados e aprovados de acordo com as normas em vigor na firma (ex: análise de risco do sistema, análise de risco do fornecedor, PIA - Privacy Impact Assessment, etc.).

1.2 Modelo de Operação

Deve ser utilizada a metodologia em vigor na firma, seguindo todas as etapas, validações e aprovações previstas, nomeadamente o cumprimento dos requisitos detalhados de segurança especificados em cada uma das *checklists* publicadas.

1.3 Glossário

- ACL – Access Control List
- SSO – Single Sign On

2 Política de Desenvolvimento Seguro

2.1 Política de desenvolvimento seguro

Os controlos de segurança nos acessos a ambientes de desenvolvimento e ambientes de testes da Deloitte Portugal devem estar em conformidade com a política de controlo de acessos da firma.

Os repositórios onde se salvaguarde a informação relacionada com o desenvolvimento ou alteração de aplicações ou sistemas que processem informação confidencial de clientes devem possuir os necessários controlos de segurança para preservar a confidencialidade, integridade e necessária disponibilidade dessa informação.

Devem ser seguidos princípios para codificação segura de acordo com os standards da firma e as melhores práticas para cada linguagem de programação e *framework* de desenvolvimento utilizados.

Os requisitos de segurança da informação devem ser estabelecidos e formalizados de análise e incluídos na fase de desenho de qualquer aplicação ou sistema que processe informação confidencial de clientes ou quando ocorre a necessidade de qualquer alteração a estes.

O projeto associado ao desenvolvimento ou melhoria de aplicações ou sistemas que processem informação confidencial de clientes deve incorporar fases específicas, em momentos apropriados, para verificação do estado de conformidade com os requisitos de controlos de segurança da informação.

Deve estar formalizado um processo que inclua as fases inerentes a todo o ciclo de vida de desenvolvimento de aplicações ou sistemas e identifique procedimentos a realizar nas fases de revisão e testes da solução.

Deve ser salvaguardada e adequadamente protegida a informação considerada necessária ao controlo das versões das aplicações ou sistemas que processem informação confidencial de clientes da firma.

Os colaboradores internos ou externos que contribuam para o desenvolvimento ou alteração de aplicações ou sistemas que processem informação confidencial de clientes devem possuir as competências necessárias que contribuam para o desenvolvimento seguro desses ambientes.

2.2 Princípios para o desenvolvimento de sistemas seguros

O desenvolvimento interno de sistemas de informação seguros, deverá ter em consideração a necessidade de:

- Analisar e incorporar, sempre que possível, componentes de segurança em todos os níveis de arquitetura (negócio, aplicações, dados e tecnologia);
- Analisar a possibilidade de incorporação de “open standards” de segurança para salvaguarda da portabilidade e interoperabilidade dos sistemas;
- Desenhar e implementar mecanismos de auditoria para deteção de utilização não autorizada e suporte a investigações de incidentes de segurança;
- Limitar, sempre que possível, o nível de privilégios atribuídos no domínio do sistema de informação;
- Balancear os controlos para proteção da confidencialidade da informação com os requisitos de acessibilidade dessa mesma informação;
- Analisar riscos de segurança de novas tecnologias a utilizar;
- Desenvolver o projeto com controlos de segurança que respondam a padrões de ataques conhecidos;
- Desenhar o sistema considerando a sua utilização em ambientes em rede, formulando controlos de segurança que enderecem múltiplos domínios, autenticando utilizadores e processos internamente e externamente ao domínio do sistema;
- Assumir que os sistemas externos são inseguros;

- Avaliar a incorporação dos presentes princípios em contratos ou acordos de prestação de serviços externos de sistemas de informação;
- Aplicar os presentes princípios no desenvolvimento de aplicações que possuam interfaces de *input* e *output* de informação confidencial de clientes.

3 Política de Gestão de Alterações

3.1 Política de Gestão de Alterações

Todas as alterações aos sistemas de informação e infraestrutura de suporte da Deloitte Portugal devem seguir o processo definido de Gestão de Alterações (incluindo alterações normais e de emergência), e requerem a devida aprovação previamente à sua implementação (podendo existir alterações pré-aprovadas).

O processo é aplicável a:

- Routers;
- Switches;
- Firewalls;
- Servidores;
- Appliances; e
- Aplicações de suporte ao negócio.

Qualquer alteração que possa provocar impacto na confidencialidade, disponibilidade e integridade dos sistemas e da informação confidencial de clientes, requer a realização de um pedido de alteração que deve ficar registado na aplicação de suporte ao processo.

Os pedidos de alteração devem ser analisados e avaliado o impacto do mesmo, em conjunto com as várias áreas/equipas envolvidas. Com base na análise efetuada o pedido pode ser aprovado ou rejeitado.

Estas alterações incluem, mas não se limitam a:

- *Upgrades firmware*;
- *Upgrades software;*
- *Upgrades hardware*;
- Alterações às configurações de servidores, *firewalls*, *switchs*;
- Instalação de *patches* e *updates*;
- Novas funcionalidades aplicacionais ou correções a funcionalidades existentes.

Sempre que possível e aplicável:

- As alterações devem ser previamente efetuadas e testadas num ambiente de teste e sujeitas à aceitação antes de serem aplicadas em sistemas de produção;
- Devem ser garantidos os procedimentos e mecanismos de *fallback* previamente à implementação da alteração;
- Deve ser atualizada a documentação de suporte aos sistemas de informação e infraestrutura que foram alvo de alterações.

A implementação das alterações deverá ser calendarizada de forma a evitar ou minimizar disrupções no negócio.

Deloitte.