Requisitos Técnicos

Arquitetura de segurança das redes e sistemas de informação

No âmbito das candidaturas ao Sistema de Apoio à Modernização e Capacitação da Administração Pública (SAMA2020)

CNCS

Introdução

O presente documento[1] visa apoiar as candidaturas ao Sistema de Apoio à Modernização e Capacitação da Administração Pública (SAMA2020), definindo os Requisitos de Arquitetura de Segurança das Redes e Sistemas de Informação que as eventuais soluções resultantes deverão adotar.

Nesse sentido, considera-se fundamental que as candidaturas incluam as evidências e documentação necessárias de modo a assegurar a respetiva conformidade dos produtos resultantes das candidaturas com os requisitos aqui enunciados.

Atendendo à constante dinâmica e evolução das ameaças às redes e aos sistemas de informação, as candidaturas devem ainda evidenciar e sustentar de que forma será garantido um elevado padrão de segurança ao longo de todo o ciclo de vida do produto, através de (mas não apenas restrito a) aspetos como:

- Existência de documentos reguladores da segurança do que for desenvolvido no âmbito da candidatura (de que as políticas e normas internas são exemplos);
- Formação periódica aos utilizadores diretamente envolvidos, visando aspetos de segurança no manuseamento e administração da solução e respetivas componentes;
- Realização, em intervalos regulares, de auditorias de segurança à solução;
- Obtenção dos riscos associados à disponibilização e exploração da solução através da realização, em intervalos regulares, da respetiva análise de risco;
- Existência de contratos de manutenção ativos que garantam o acesso a atualizações que permitam corrigir de forma atempada as potencias falhas de segurança detetadas;
- Definição e execução de uma política de atualização da solução e seus componentes, com eventuais prioridades distintas face à criticidade da correção envolvida.

Nota

FE – Front-end;

App – Camada Aplicacional

BD – Camada de Base de Dados

[1] Igualmente disponível em https://www.cncs.gov.pt/content/files/SAMA2020_RASRSI_CNCS.pdf

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Requisito geral		Requisitos Específicos	Classificação
As aplicações cliente (exemplo, *Android,* IOS, WEB) devem ser desenvolvidas adotando práticas de desenvolvimento seguro.	FE	Seguir as boas práticas de desenvolvimento. Exemplo: *Open Web Application Security Project* (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório
		Utilizar sessões seguras com protocolo de Segurança.	Obrigatório
		Usar *Transport Layer Security* (TLS), na sua versão mais recente.	Recomendado
		Não guardar informação pessoal no *browser*, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório
	App	Utilizar sessões seguras com protocolo de Segurança.	Obrigatório
		Usar TLS, na sua versão mais recente, na comunicação com as camadas adjacentes.	Recomendado
		Utilizar certificados através de *Application Programming Interface* (API), não sendo desta forma necessário o uso de palavras-passe.	Recomendado
		Não utilizar credenciais em *plain text*, quer no código quer em ficheiros de configuração	Obrigatório
		Evitar palavras-passe embebidas no código.	Recomendado
		Codificar as credenciais que necessitem de ser armazenadas em ficheiros de configuração (HASH - mínimo SHA 256).	Recomendado
	BD	Garantir que a comunicação com camada aplicacional é feita através de autenticação por certificado válido por período não superior a 2 anos, no caso de as camadas serem física ou logicamente distintas. Exemplo: padrão X.509, da ITU-T para Infraestruturas de Chaves Públicas (ICP).	Obrigatório
		Prever cifra de informação pessoal (recomenda-se mínimo 2048 bit) apenas se a aplicação cliente tiver camada de BD física e logicamente distinta, usando preferencialmente tecnologia que permita interoperabilidade entre sistemas.	Obrigatório
Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações.	FE	Iniciar e manter sempre o processo de autenticação em sessão segura.	Obrigatório
		Utilizar: 1) TLS, na sua versão mais recente; ou 2) palavra-passe, preferencialmente em combinação com outro fator (*Double Factor Authentication* -2FA), como por exemplo: – Palavra-passe + SMS *Token*	Recomendado

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

		– Palavra-passe + *Smartcard* – Palavra-passe + Biometria – Palavra-passe + padrão gráfico – Palavra-passe + Cartão de coordenadas – Palavra-passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-*Code*.	
		Excluir os dados pessoais de sessão das variáveis *Uniform Resource Locator* (URL) ou de outras variáveis visíveis ao utilizador.	Obrigatório
		Transmitir as credenciais de início de sessão através do seu *HASH*, mínimo *Secure Hash Algorithm*- 256 (SHA-256), ou utilizar cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra-passe em *HASH* e restantes dados cifrados).	Obrigatório
		Garantir que, sempre que aplicável, a palavra-passe tenha, no mínimo, 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de "espaço".	Obrigatório
		Para novos sistemas utilizar como padrão de autenticação o 2FA.	Recomendado
	App	Garantir que a palavra-passe dos administradores tenha, no mínimo, 13 caracteres e seja complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de "espaço".	Obrigatório
		Garantir que, para todos os administradores, seja usado como padrão de autenticação o 2FA: Exemplos: – Palavra-passe + *Smartcard* – Palavra-passe + Biometria – Palavra-passe + certificado (por exemplo X.509, da ITU-T para ICP, válido por período não superior a 2 anos).	Obrigatório

		Utilizar o *Token* como mecanismo de proteção e segurança da informação.	Recomendado
		Efetuar a comunicação com camadas FE ou BD através de sessão segura com prévia autenticação, se as camadas forem física ou logicamente distintas.	Obrigatório
		Evitar palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (*HASH*, mínimo SHA- 256).	Recomendado
		Utilizar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado
		Garantir que a autenticação dos elementos comunicantes é efetuada por validação de informação estática ao nível da rede. Exemplos: 1) utilização de IP fixo + *hostname* + *MacAddress* + fatores de autenticação, ou 2) Utilização de certificados.	Obrigatório
	BD	Garantir que a palavra-passe tenha, no mínimo, 13 caracteres e seja complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de "espaço".	Obrigatório
		Transmitir os dados pessoais de autenticação através do seu *HASH* (mínimo SHA-256), ou recorrer à cifra ou codificação para efetuar essa transmissão.	Recomendado
Atribuição de direitos de acesso e privilégio de forma restrita e controlada.	FE	Criar perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (*Create, Read, Update, Delete* - CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		Criar registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório
	App	Criar perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

		Criar registo de acesso, alteração e remoção (*logs*) com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório
	BD	Criar perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer. Criar registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório Obrigatório
Atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida.	FE	Definir processo de acordo com uma política de "Atribuição de direitos de acesso e privilégio de forma restrita e controlada". Atribuir credenciais de acesso de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação. Exemplo: – Enviar informação de autenticação por SMS com validade limitada (não superior a 5 minutos), com primeiro acesso a implicar sempre a redefinição da informação enviada; – Enviar informação de autenticação gerada automática e aleatoriamente, enviada por Envelope (semelhante ao do envio de dados do Cartão de Cidadão).	Obrigatório Obrigatório
	App	Definir processo de acordo com uma política de "Atribuição de direitos de acesso e privilégio de forma restrita e controlada". Atribuir credenciais de acesso de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação ou do auditor.	Obrigatório Obrigatório
	BD	Definir processo de acordo com uma política de "Atribuição de direitos de acesso e privilégio de forma restrita e controlada". Atribuir credenciais de acesso de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação ou do auditor.	Obrigatório Obrigatório

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Revisão de direitos de acesso de utilizadores em intervalos regulares.	FE	Definir processo de renovação de conta do utilizador, de acordo com os mesmos requisitos de segurança da criação do mesmo, não devendo ter um ciclo de vida superior a 180 dias.	Obrigatório
		Gerir o ciclo de vida da conta do utilizador tendo em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
		Desativar uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses.	Recomendado
	App	Definir processo de gestão de validade de perfis.	Obrigatório
		Definir processo de gestão de validade de perfis automatizado.	Recomendado
		Definir processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo, bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
	BD	Definir processo de gestão de validade de perfis.	Obrigatório
		Definir processo de gestão de validade de perfis automatizado.	Recomendado
		Definir um processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo, bimestral ou quando se verifique uma	Obrigatório

		alteração no mapa de pessoal associado a esta função.	
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados.	FE	Gerir o ciclo de vida da conta do utilizador tendo em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta de utilizador é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
		Auditar a ação dos utilizadores sobre dados pessoais (CRUD) em registo de atividade (*logs*).	Obrigatório
	App	Aplicar os requisitos da camada FE a Administradores de Bases de Dados, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais .	Obrigatório
		Definir processo de gestão de validade de contas de utilizadores.	Obrigatório
		Definir processo de gestão de validade de contas de utilizadores automatizado.	Recomendado
		Definir processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade limitada.	Obrigatório
		Recomenda-se: 1) uma periocidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
	BD	Aplicar os requisitos da camada FE a Administradores de Bases de Dados, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais.	Obrigatório

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

		Definir processo de gestão de validade das contas dos utilizadores.	Obrigatório
		Definir processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado
		Configurar alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil).	FE	Associar a tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
	App	Associar a tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		Definir processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização	Obrigatório
	BD	Associar a tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório
		Definir processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório
Automatização dos processos de concessão, revisão, análise e revogação de acesso.	Aplicar as mesmas disposições que em "Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados" e "Revisão de direitos de acesso de utilizadores em intervalos regulares".		Obrigatório

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Procedimentos seguros de início de sessão.		Aplicar as mesmas disposições referidas em "Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o acesso controlado por um procedimento seguro de início de sessão".	Obrigatório
Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis.		Guardar registo de atividade (*log*) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.	Obrigatório
		Armazenar todos os registos de atividade (*log*) apenas em modo de leitura, devendo, com uma periodicidade máxima de 1 mês, ser englobados num único bloco de registos e assinado digitalmente (garantia de integridade).	Obrigatório
		Guardar o registo de atividade (*log*) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.	Obrigatório
		Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, *browsers*, Sistema de Gestão de Base de Dados - SGBD, etc.) são inequivocamente associados à sua origem.	Obrigatório
		Os registos de atividade (*log*) devem conter, no mínimo, o endereço de acesso (IP e Porto), *Host*, *HASH* da conta do utilizador que efetuou a ação, ação efetuada (CRUD), Tipo de Dado Pessoal onde a ação foi efetuada, data/hora/minuto/segundo (*TimeStamp*) da ação, alteração efetuada sobre o dado pessoal.	Obrigatório
Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional.		A entidade responsável pela segurança dos dados deve definir e implementar mecanismos de proteção da informação em função da sua relevância e criticidade: – Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas *firewall*, *Intrusion Detection System* - IDS, etc.); – Extensão desta proteção desejavelmente a todos os dispositivos (incluindo móveis) com acesso a dados pessoais nos sistemas corporativos; – Mecanismo de cifra ponto a ponto sempre que houver necessidade de aceder remotamente ao FE (e apenas a esta camada), como por exemplo com recurso à tecnologia *Virtual Private Network* (VPN).	Obrigatório
Proteção dos dados contra modificações não autorizadas, perdas, furtos e divulgação não autorizada.	FE	Desenvolver e colocar em produção o FE de acordo com as melhores práticas de segurança, garantindo a proteção desta camada aos ataques mais comuns (SQLi, injeção de código, etc.).	Obrigatório

		Seguir as práticas recomendadas em *Open Web Application Security Project* (OWASP)	Recomendado
		Aplicar as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório
	App	Segregar a camada aplicacional da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório
		Aplicar as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório
	BD	Segregar a camada de BD da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório
		Aplicar as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório
		Mascarar, anonimizar ou, sendo necessário, cifrar os dados pessoais transmitidos ou acedidos.	Obrigatório
		Cifrar e assinar digitalmente os dados armazenados (incluindo os existentes em volumes de salvaguarda - *backups*).	Recomendado
		Efetuar o armazenamento de dados pessoais considerados muito críticos de forma fragmentada e em locais físicos distintos, mantendo-se todavia a sua unicidade e integridade lógica.	Recomendado
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais.		Garantir a integridade das zonas *Domain Name System* (DNS) onde se encontra inserido o sistema e o ecossistema envolvente, recorrendo às boas práticas de DNSSec e de configuração de sistemas de Correio Eletrónico (por exemplo, *Sender Policy Framework* - SPF, *DomainKeys Identified Mail* – DKIM, *Domain-based Message Authentication, Reporting and Conformance* - DMARC, entre outros).	Obrigatório
		Utilizar tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de	Recomendado

	ambientes tecnológicos distintos seja efetuada em segurança.	
Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum "*single point of failure*".	A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório
	Garantir a existência de dois tipos de *backups* (*online* e *offsite*), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório
	Armazenar os *backups offsite* numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização mas geograficamente distinta e/ou afastada.	Obrigatório
As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais.	Garantir a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços, adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutro que o venha a substituir.	Obrigatório

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt