Requisitos Mínimos de Segurança para as Unidades de Registo da Infraestrutura de Chaves Publicas de Cabo Verde

1. DISPOSIÇÕES GERAIS

1.1. Este documento tem por finalidade regulamentar os procedimentos mínimos a serem adotados pelas Unidades de Registo (UR) da Infraestrutura de Chaves Publicas de Cabo Verde (ICP-CV). O presente regulamento tem por finalidade complementar as disposições referentes à segurança das URs constantes dos documentos Requisitos Mínimos de Redação para Declaração de Práticas de Certificação (DPC) e a Política de Segurança vigentes no Âmbito da ICP-CV.

1.2. As normas de segurança aplicam-se a todas as URs integrantes da ICP-CV e devem ser observadas em todas suas instalações técnicas.

1.3. Os critérios e procedimentos para credenciamento de uma UR e para abertura de novas instalações técnicas de UR já credenciada estão definidos no documento Procedimentos para credenciamento na ICP-CV.

1.4. No âmbito da ICP-CV somente poderão emitir solicitação de certificados as URs cujas aprovações de credenciamento foram publicadas no Boletim Oficial e que suas instalações técnicas estejam igualmente autorizadas a funcionar nos mesmos termos.

1.5. A alteração de endereço da instalação técnica deve ser previamente reportada à EC (Entidade de Certificação) responsável pela UR, que por sua vez deve enviar à Autoridade Credenciadora da ICP-CV o formulário de solicitação de credenciação, requerendo nova autorização de funcionamento, que deve ser acompanhado dos documentos previstos no documento Procedimentos para credenciamento na ICP-CV.

1.6. O cumprimento das regras constantes deste documento será verificado por meio de auditorias e fiscalizações, realizadas consoante documento Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-CV.

2. SEGURANÇA DE PESSOAL

2.1. Disposições Gerais

2.1.1. As normas internas das UR devem abranger os aspectos seguintes: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por acções não autorizadas, controlos para contratação e documentação sobre os processos de certificação digital.

2.1.2. Os contratos ou termos de responsabilidade dos encarregados de tarefas operacionais devem abranger os aspetos seguintes:

a) Os termos e as condições operacionais do perfil;

b) Compromisso de cumprir as normas, políticas e regras aplicáveis da ICP-CV; e

c) Compromisso de não divulgar informações sigilosas.

2.1.3 O pessoal que desempenha funções nas URs deve possuir suficientes qualificações para desempenhar a função e deve ser submetido a:

a)Verificação de antecedentes criminais;

b)Verificação de histórico de empregos anteriores; e

c)Comprovação de escolaridade e de residência.

2.1.4 A UR deve implementar um plano de formação e treino, que engloba os seguintes tópicos:

a)Certificação digital e Infra-estruturas de Chaves Publicas;

b)Conceitos gerais sobre a segurança da informação;

c)Formação específica para o seu posto;

d)Funcionamento do *software* e/ou *hardware* usado pela EC;

e)Política de Certificados e Declaração de Práticas de Certificação;

f)Recuperação face a desastres;

g)Procedimentos para a continuidade da actividade;

h)Aspectos legais básicos relativos à prestação de serviços de certificação;

i)A Politica de Segurança implementada.

2.1.4. No âmbito da ICP-CV não são admitidos estagiários nem funcionários terceirizados no exercício das atividades de Agente de Registo. Os Agentes de Registo devem ser trabalhadores ou funcionários da entidade credenciada como UR.

2.1.5. O acesso do Agente de Registo aos sistemas da EC só é concedido pela EC vinculada à UR, após a receção de toda a documentação do referido Agente.

2.1.6. A UR deve enviar à EC a relação atualizada dos Agentes de Registo em atividade, seus perfis qualificados e suas necessidades de acesso às informações de administração do ciclo de vida dos certificados. A EC deve manter essa informação atualizada, consolidada e organizada por instalação técnica, inclusive com o histórico das alterações realizadas, à disposição da Entidade Credenciadora e atendendo aos princípios facilitadores de auditoria e fiscalização.

2.2. Documentação do Agente de Registo

2.2.1. Cada Agente de Registo que atua na UR deve possuir um dossiê, que deve ser conservado mesmo após seu desligamento da UR, contendo:

a) Contrato de trabalho onde consta o registo da contratação, nomeação no boletim oficial ou comprovativo de situação laboral;

b) Comprovativo da verificação de antecedentes criminais;

c) Currículo com histórico de empregos anteriores;

d) Comprovação de grau de escolaridade e de residência;

e) Comprovativo das formações realizadas em Certificação Digital;

f) Declaração em que o Agente de Registo afirma conhecer as suas atribuições e em que assume o dever de cumprir a Política de Segurança da EC e as políticas e regras aplicáveis da ICP-CV;

g) Declaração em que o Agente de Registo assume o dever de manter a confidencialidade e exclusividade de propriedade das informações disponibilizadas pela EC à UR e de manter sigilo, mesmo quando desligado da UR, sobre todas as informações e os processos executados na UR;

h) Documento que dispõe sobre o resultado da avaliação periódica e as necessidades de formação e avaliação do funcionamento do sistema de segurança, previstos na Política de Segurança da EC;

i) Cópia do documento, criado em meio digital ou em papel, que comprove que a UR solicitou à EC a habilitação do Agente de Registo no sistema de certificação.

2.2.2. Caso o Agente de Registo tenha sido desligado de suas atividades na UR, seu dossiê deve conter, também:

a) Cópia do documento, criado em meio digital ou em papel, que comprova que a UR solicitou à EC a revogação dos diretos de acesso ao sistema de certificação do Agente de Registo;

b) Documento da EC que comprova a realização da revogação dos direitos de acesso do Agente de Registo solicitado na alínea a).

2.2.3.Para habilitação de acesso ao sistema de certificação da EC o dossiê do Agente de Registo deve ser examinado por uma das pessoas abaixo indicadas, que deve declarar, sob as penas da lei, a existência de comprovativo de que o Agente de Registo atende a todos os requisitos solicitados, que são pertinentes à função que exerce no âmbito da ICP-CV:

a) Auditor ou funcionário designado para o efeito, com vinculo contratual à EC responsável pela UR;

b) Representante legal da própria UR.

2.2.4. Somente após a receção da solicitação de habilitação do Agente de Registo e da declaração prevista no item anterior, a EC pode conceder as permissões de acesso no sistema de certificação.

2.2.5. Os dossiês de todos os Agentes de Registo da UR devem ficar em um local de arquivo central pertencente à UR, com conhecimento de sua localização pela Autoridade Credenciadora, para fins de auditoria e fiscalização.

2.3. Formação

2.3.1. Todo o Agente de Registo, na ocasião de sua admissão nessa função, deve receber formação e documentação sobre os seguintes temas:

a) Certificação Digital e Infraestrutura de Chave Publica;

b) Conceitos gerais sobre segurança da informação;

c) Formação específica para o seu posto;

e) Política de Certificados e Declaração de Práticas de Certificação;

f) Procedimento para a continuidade da atividade;

g) Aspetos legais básicos relativos à prestação de serviços de certificação.

2.3.2. Na formação sobre os princípios e mecanismos de segurança devem ser apresentados a Política de Segurança da EC, suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de se desenvolver e manter uma efetiva consciencialização sobre segurança, assim como instruir o seu fiel cumprimento.

2.3.3. Preferencialmente, o Agente de Registo deve ter formação em reconhecimento de assinaturas e validade dos documentos apresentados. Essa formação deve ser ministrada (ou preparada, quando se tratar de formação do tipo e-learning) por empresa ou profissional especializado em grafotecnia.

2.4. Acompanhamento periódico

2.4.1. A UR deve acompanhar o desempenho das funções de seus Agentes de Registo e proceder a uma avaliação anual com o propósito de detetar a necessidade de atualização técnica e de segurança. Esse processo deve ser documentado.

2.4.2. A UR deve realizar as verificações de antecedentes criminais para todos os seus Agentes de Registo, com periodicidade de cinco anos.

2.4.3. Se o acompanhamento anual identificar a necessidade de suspensão do Agente de Registo, o responsável pela UR deve de imediato solicitar à EC suspensão dos direitos de acesso do Agente de Registo aos sistemas da UR, em definitivo ou até a supressão das necessidades identificadas.

2.4.4. A UR deve arquivar os comprovativos relativos aos procedimentos de suspensão no dossiê dos Agentes de Registo em seu poder.

2.5. Suspensão e Desligamento

2.5.1. Quando o Agente de Registo é suspenso ou desligado de suas atividades, a UR deve imediatamente providenciar a revogação de suas permissões de acesso ao sistema de certificação da EC e permissões de acesso físico e lógico aos equipamentos e mecanismos inerentes à atividade de Agente de Registo. Esses processos devem ser documentados e esses documentos devem ser arquivados no dossiê do Agente, em poder da UR.

2.5.2. A UR deve solicitar à EC a revogação das permissões de acesso ao sistema de certificação, informando o motivo da suspensão ou desligamento do Agente de Registo. O responsável designado para essa tarefa deve expedir uma ordem de revogação da permissão de acesso ao sistema. Esses processos devem ser documentados e arquivados no dossiê do Agente de Registo.

3. SEGURANÇA FÍSICA

3.1. As instalações técnicas e os postos provisórios de uma UR podem ser de 2 tipos:

a) Ambiente dedicado às atividades da UR;

b) Ambiente compartilhado com outras atividades da organização.

3.2. Para ambos os casos, aplicam-se as seguintes exigências mínimas de segurança:

a) Equipamentos de combate a incêndios;

b) Armário ou gabinete com chave, de uso exclusivo da UR, para a guarda de documentos da UR (em especial Termos de Titularidade);

c) Circuitos elétricos de alimentação dos equipamentos de processamento de dados que devem ser protegidos por no-break ou estabilizador de tensão;

d) Circuitos elétricos e lógicos que deverão ser protegidos por tubulação e/ou calhas adequadas.

3.3. Para as URs que possuem ambiente dedicado, aplicam-se, além das exigências do item 3.2, as seguintes:

a) Controle de acesso ao ambiente, com autorização de acesso apenas para os agentes de registo e titulares de certificados;

b) Porta única de entrada, com fechadura tetra;

c) Paredes e tetos constituídos em alvenaria de tijolos ou de material de resistência equivalente;

d) Iluminação de emergência.

OBS.: Caso a sala possua janelas ou qualquer outra abertura para o ambiente externo do prédio, essas devem ser lacradas ou gradeadas, para impedir o acesso externo.

3.4. Para as UR que possuem ambiente compartilhado aplicam-se, além das exigências do item 3.2, também as seguintes:

a) Vigilância ostensiva ou videovigilância no interior do ambiente da UR;

b) Controle de acesso ao prédio ou ao ambiente onde está instalada a UR.

3.5. A videovigilância pode ser realizada pela própria UR ou por empresa de segurança contratada. A câmara deve filmar o ambiente e equipamentos da UR e as imagens devem ser mantidas por 15 dias, em ambiente seguro.

3.6. As atividades da UR relativas a validação da solicitação de certificados podem ser executadas externamente ao ambiente da UR, desde que sejam utilizados para tal equipamentos portáteis que atendam aos requisitos de segurança do item 4.

3.7 Os equipamentos portáteis devem ser fechados a chave e durante o seu transporte devem estar sempre desligados e acompanhados por dois Agentes de Registo credenciados, sendo um responsável pela chave e o outro responsável pelo equipamento.

4. SEGURANÇA LÓGICA

4.1. Estações de trabalho

4.1.1. As estações de trabalho da UR, incluindo equipamentos portáteis, devem estar protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos.

4.1.2. As estações de trabalho da UR, incluindo equipamentos portáteis, devem receber, pelo menos, as seguintes configurações de segurança:

a) Controle de acesso lógico ao sistema operacional;

b) Exigência de uso de senhas fortes;

c) Diretivas de senha e de bloqueio de conta;

d) Logs de auditoria do sistema operacional ativados, com registo dos eventos seguintes:

i. Iniciação e encerramento do sistema;

ii. Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da UR;

iii. Mudanças na configuração da estação;

iv. Tentativas de acesso (login) e de saída do sistema (*logoff*);

v. Tentativas não-autorizadas de acesso aos arquivos de sistema;

vi. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves;

e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;

f) *Firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

g) Proteção de tela acionada no máximo após dois minutos de inatividade e exigência de senha do usuário para desbloqueio;

h) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches, hotfix*, etc.);

i) Utilização apenas de *softwares* licenciados e necessários para a realização das atividades do usuário;

j) Impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela UR, exceto para as atividades de suporte remoto.

4.1.3. Os *logs* de auditoria do sistema operacional devem registar os acessos aos equipamentos e devem ficar armazenados localmente por um período mínimo de 60 (sessenta) dias.

4.1.4. A análise desses *logs* deve ser realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

4.1.5. O Agente de Registo não deve possuir perfil de administrador ou senha de root dos equipamentos, ficando essa tarefa delegada a terceiros da própria organização, para permitir segregação de funções.

4.2. Aplicativo da UR

4.2.1. O aplicativo que faz interface entre a UR e o sistema de certificação da EC deve possuir pelo menos as seguintes características de segurança:

a) Acesso permitido somente mediante autenticação por meio de certificado de Assinatura Qualificada, nos moldes do Decreto-Lei n.º 33/2007, de 24 de Setembro;

b) Acesso permitido somente a partir de equipamentos autenticados no sistema da EC (ex. usando registo prévio de endereço IP, certificado digital de equipamento ou outra solução que permita ao sistema identificar de forma inequívoca o equipamento);

c) Time out de sessão de acordo com a análise de risco da EC;

d) Registo em log de auditoria dos eventos citados no item 7.10.3 do documento Requisitos Mínimos de Redação para Declaração de Práticas de Certificação (DPC) no Âmbito da ICP-CV;

e) Registo do histórico da inclusão e exclusão dos Agentes de Registo no sistema e das permissões concedidas ou revogadas;

f) Registo em log, para cada certificado emitido, informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da UR;

g) Mecanismo para revogação automática dos certificados digitais emitidos fora do ambiente da UR e que não tenham sido verificados pelo segundo Agente de Registo, mediante cópia da documentação apresentada na etapa de validação, até o momento do início da validade do certificado.

4.2.2. Para atender às disposições do item 9.1 do documento Requisitos Mínimos de Redação para Declaração de Práticas de Certificação (DPC) no Âmbito da ICP-CV, o aplicativo da EC deve:

a) Ser desenvolvido com documentação formal;

b) Ter mecanismos para controle de versões;

c) Ter documentação dos testes realizados em cada versão;

d) Ter documentação comprovando a homologação de cada versão em ambiente com as mesmas características ambiente de produção, sendo esses ambientes, porém, obrigatoriamente independentes entre si;

e) Ter aprovação documentada do gerente da EC, ou responsável designado, para colocar cada versão em ambiente de produção.

4.2.3. Os *logs* gerados pelo aplicativo devem ser armazenados na EC pelo prazo de 20 anos, conforme previsto no item 7.11.3 do documento Requisitos Mínimos de Redacção para Declaração de Práticas de Certificação (DPC) no Âmbito da ICP-CV.

5. SEGURANÇA DE REDE

5.1. Cada instalação técnica deverá elaborar diagrama da topologia de rede de comunicação entre a UR e a EC, que deve ser mantido sempre atualizado. Esse documento deve estar arquivado no dossiê que contém os documentos sobre a instalação técnica.

5.2. A UR deve encaminhar as solicitações de emissão ou de revogação de certificados à EC utilizando VPN (Virtual Private Network), SSL (Secure Socket Layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.

6. SEGURANÇA DA INFORMAÇÃO

6.1. Diretrizes Gerais

6.1.1. Cada instalação técnica deve possuir um dossiê, contendo cópia dos seguintes documentos, atualizados:

a) Relação dos Agentes de Registo que atuam ou já se desligaram da UR com respetivo nº de NIF;

b) Topologia de Rede de Comunicação entre a UR e a EC;

c) Manual Operacional dos Agentes de Registo;

d) Inventário de Ativos;

e) Plano de Continuidade de Negócios (opcional);

f) Análise de Risco (opcional).

6.1.2. Se houver um Plano de Continuidade de Negócios deve-se manter uma cópia do mesmo em local seguro, fora da sala da UR.

6.1.3. O Inventário de Ativos deve estar sempre atualizado, mantendo histórico das alterações e deve ser assinado pelo responsável pela instalação técnica ou posto provisório.

6.1.4. O Inventário de Ativos deve relacionar, pelo menos:

a) Equipamentos da UR, com respetivas especificações, atualizado mensalmente;

b) *Softwares* instalados nos equipamentos atualizado mensalmente.

6.2. Armazenamento, manuseio, guarda e destruição de documentos

6.2.1. Os documentos em papel que compõem os dossiês dos titulares de certificados e da instalação técnica devem ser guardados, obrigatoriamente, num armário com chave e com acesso permitido somente aos Agentes de Registo.

6.2.2. A UR pode substituir a guarda física dos documentos que compõem o dossiê do Agente de Registo e o dossiê do Titular do Certificado por digitalização dos mesmos, desde que sejam observados o seguinte:

a) As cópias dos documentos que compõem o dossiê (ex.: documentos de identificação apresentados pelo titular, cópia de contrato social etc.) devem ser digitalizadas e assinadas digitalmente com o certificado da ICP-CV do agente de Registo;

b) Documentos cujo original deva constar do dossiê (ex.: termos de titularidade, declarações do Agente de Registo etc.) podem ser digitalizados para inclusão no dossiê

respetivo, mas os originais não podem ser destruídos, devendo permanecer arquivados na UR ou EC pelo prazo de mínimo de vinte anos;

c) Todos os arquivos que compõem os dossiês devem ser organizados de forma a permitir sua recuperação conjunta, para fins de fiscalização e auditoria;

d) O diretório ou sistema onde são armazenados esses arquivos deve ter proteção conforme previsto na Lei n.º 41/VIII/2013, de 17 de Setembro, que altera a Lei n.º 133/V/2001, de 22 de Janeiro, que aprova o regime jurídico de proteção de dados pessoais das pessoas singulares;

e) Devem ser especificados procedimentos de cópia e recuperação em caso de desastre.

6.2.3. O arquivo em definitivo dos dossiês de titulares de certificado, em papel ou digitalizados, deve ser feito na própria UR ou na EC à qual a UR está vinculada.

6.2.4. O critério de cada UR, pode ser mantida cópia do dossiê na instalação técnica onde foi gerado, sem prejuízo da obrigatoriedade de guarda do documento original num dos locais supra citados.

6.2.5. A remessa ou transmissão do dossiê para o arquivo definitivo deve ser feita por meio seguro (ex.: para documentos em papel transporte com escolta de dois funcionários em veiculo próprio da entidade e transmissão via VPN para documentos digitalizados), no prazo máximo de 30 dias corridos, a partir da criação do dossiê.

6.2.6. A UR deve utilizar sistema que permite determinar, facilmente e a qualquer momento, o local onde se encontra cada dossiê de titular de certificados que se encontra sob sua guarda.

6.2.7. O local de arquivo dos dossiês, na EC ou na UR, deve possuir requisitos de segurança física e/ou lógica no mínimo equivalente ao de uma instalação técnica de UR e sua localização deve ser informada à Autoridade Credenciadora, bem como qualquer alteração que venha a ser feita posteriormente.

6.2.8. O descarte dos documentos em papel que contêm informações classificadas como sensíveis deve ser feito de forma a tornar irrecuperável a informação neles contidos, antes de ir para o lixo. Incluem-se nessa categoria cópias não utilizadas de documentos dos titulares de certificados, termos de titularidade descartados, diagramas de rede etc.

6.2.9. A exclusão de arquivos digitais contendo cópias de documentos dos dossiês de titulares de certificados deve contemplar o descarte completo, inclusive com limpeza da lixeira, de forma a impedir sua recuperação e uso indevidos.

7. CICLO DE VIDA DO CERTIFICADO

7.1. Os processos que dizem respeito ao ciclo de vida do certificado - solicitação, validação e verificação da solicitação, emissão e revogação - estão descritos nos itens 6 e 7 do documento Requisitos Mínimos de Redação para Declaração de Práticas de Certificação (DPC) no Âmbito da ICP-CV.

8. ACRÓNIMOS

CCTV	Circuito Fechado de Televisão

CG	Comité Gestor
DPC	Declaração de Práticas de Certificação
EC	Entidade Certificadora
ICP-CV	Infraestrutura de Chaves Públicas de Cabo Verde
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócios
PIN	*Personal Identification Number*
PS	Política de Segurança
SSL	*Secure Socket Layer*
UR	Unidade de Registo