



NORMA TÉCNICA – D 02

REQUISITOS MÍNIMOS DE SEGURANÇA FÍSICA DE INSTALAÇÕES DE ENTIDADES CERTIFICADORAS

Lisboa, 02 de dezembro de 2024

A Autoridade Nacional de Segurança

(António Gameiro Marques)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

1. REFERÊNCIAS

Nada a referir

2. SITUAÇÃO

Sendo as Entidades Certificadoras (EC) o elemento fundamental das infraestruturas de chaves públicas, muita da sua credibilidade assenta no grau de proteção da sua instalação física.

De uma forma generalista, se um servidor não está instalado num ambiente seguro, toda a infraestrutura pode ser comprometida.

Levando em conta esta premissa, a atividade operacional de uma EC transcende a simples implementação de um pacote de software e hardware, daí que a segurança do ambiente onde estas entidades disponibilizam os seus serviços, deverá ser alvo de particular atenção e estar assente num projeto abrangente, materializando a integração de medidas de segurança física, eletrónica, de pessoal e administrativas.

3. OBJECTO / FINALIDADE

A presente norma incide nos aspetos de segurança física das instalações onde operam as EC, de modo a assegurar a manutenção da integridade, fiabilidade e confiança dos serviços por estas prestados.

Tendo em consideração que as instalações dos Órgãos que atuam como EC nem sempre são exclusivas da atividade de EC, a aplicação destes requisitos visa regulamentar as medidas de segurança mínimas a serem aplicadas ao local e edifício como um todo, permitindo assim que as atividades se realizem de forma segura.

4. ÂMBITO

A presente norma aplica-se às Entidades Certificadoras, Entidades de Validação Cronológica e Auditores de Segurança de Entidades Certificadoras.

5. EXECUÇÃO

a. Introdução

Os requisitos descritos nesta norma têm em linha de conta a conceção, construção e localização das Zonas de Alta Segurança e respetivos sistemas, nomeadamente, controlo de acessos, deteção de intrusões, deteção e extinção de incêndios, sistemas elétricos e energia alternativa, ar condicionado, inundações, entre outros.

As instalações das EC devem ser desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, devendo estar fisicamente protegidas do acesso não autorizado, do dano ou da interferência. Esta proteção pode ser incrementada proporcionalmente sempre que a avaliação de risco assim o justificar.

Em termos de construção, é exigido que a infraestrutura de perímetro, nomeadamente, as paredes, pavimento, teto, janelas, sejam constituídos por materiais com um nível de resistência igual ou superior ao definido para as respetivas portas de acesso. Desta forma garante-se um nível de resistência uniforme, que visa proporcionar a adequada proteção física contra ações de intrusão de acordo com o quadro de ameaças vigente. A arquitetura deverá ser criada aplicando o conceito de defesa em profundidade, diferenciados e com graduais incrementos de segurança. O acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

Esta premissa assenta na existência complementar e integrada de um conjunto de subsistemas, que juntos, formam um Sistema Complementar de Segurança (SCS), de funcionamento ininterrupto, proporcionando um ambiente seguro, em que os vários subsistemas devem possuir a máxima integração que a tecnologia possibilite, de forma a se comportar como um único sistema em que a resposta individualizada de um subsistema deve provocar uma resposta complementar dos restantes.

O SCS deverá ser composto, no mínimo, pelos seguintes subsistemas:

- 1) Subsistema de Controlo de Acessos (SCA);
- 2) Subsistema de Detecção de Intrusão (SDI);
- 3) Subsistema de Videovigilância (SVV);
- 4) Subsistema Automático de Detecção de Incêndios e Alerta (SADI)
- 5) Subsistema Automático de Detecção e Extinção de Incêndios (SADEI);

A figura 1 ilustra uma representação gráfica do ambiente global pretendido, apresentando uma planta de um edifício situado num local não acessível, de forma direta à intrusão (p.e.: 2.º piso), quer por meios humanos (p.e.: entrada furtiva), quer por meios físicos (p.e.: arrombamento de portas ou janelas, quebras de vidros, utilização de condutas ou aberturas, bem como outras ações de violação do perímetro).

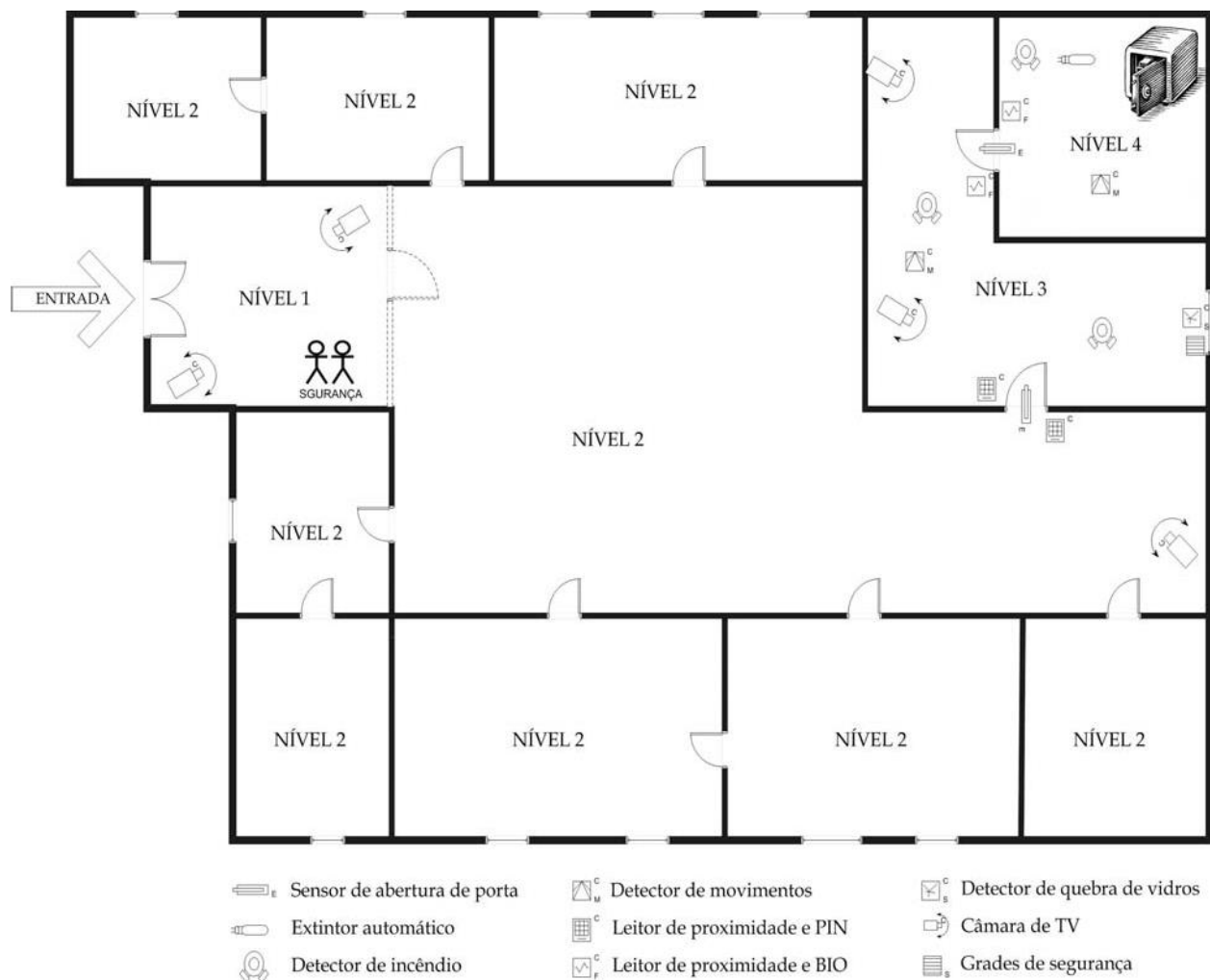


Figura 1 – Ambiente global de segurança

b. Descrição dos níveis de segurança

De seguida, apresentam-se as características a que deverão obedecer os diferentes níveis de segurança que constituem o ambiente seguro onde operam as EC. Os níveis apresentados aparecem por ordem crescente de importância, devendo ser entendidos como os níveis mínimos exigidos.

1) Nível de segurança 1

- Este nível constitui-se como o primeiro perímetro de segurança, materializa-se pela entrada e zona de receção do edifício.
- É requerida a utilização de um Subsistema de Controlo de Acessos e de um Subsistema de Videovigilância.
- Subsistema de Controlo de Acessos
 - No acesso às instalações, todo o pessoal afeto à Organização está sujeito às medidas de segurança que estiverem definidas pelas políticas de segurança implementada pela Entidade/Organização.
 - Os visitantes aquando do acesso às instalações, deverão ser submetidos ao processo de identificação/confirmação da identidade, registo e controlo de segurança pelo efetivo de Segurança da Organização, ao que posteriormente

deverão ser rececionados e acompanhados por pessoal afeto à Organização.

d) Subsistema de Videovigilância

- (1) Esta zona deverá estar munida de câmaras de videovigilância, capazes de monitorizar todos os pontos de acesso ao edifício;
- (2) Antes da entrada nas instalações deve encontrar-se afixada em local bem visível a informação de que o local se encontra com proteção de videovigilância para propósitos de segurança.

2) Nível de segurança 2

- a) Este nível constitui-se como o segundo perímetro de segurança e é materializado pela zona de trabalho global da Organização (p.e.: zona das salas de trabalho).
- b) A circulação dentro deste nível é permitida ao pessoal afeto à Organização e com as necessárias credenciais de acesso, de acordo com a metodologia de identificação e controlo utilizada no nível anterior.
- c) A circulação de visitantes dentro desta área, requer o acompanhamento permanente da parte de pessoal afeto à Organização.

3) Nível de segurança 3

- a) Este nível é uma zona de antecâmara para as instalações da EC, pelo que:
 - (1) É uma zona de acesso ainda mais restrito, servindo de zona tampão ao Nível de segurança 4;
 - (2) Esta área garante que o pessoal que circula na zona de trabalho (Nível de segurança 2), não circule nas imediações da entrada que possibilita o acesso ao Nível de segurança 4;
 - (3) O acesso a esta área apenas é permitido a pessoal com autorização expressa permanente, decorrente das suas funções na estrutura da EC (incluindo o pessoal da Organização afeto aos serviços de suporte e apoio);
 - (4) Os visitantes circulam dentro desta área, apenas sob acompanhamento do pessoal da Organização autorizado conforme o §(3) e com prévia autorização.
- b) Características e tipo de construção da área:
 - (1) As paredes do perímetro exterior: Devem ser de construção sólida e resistente, com recurso a materiais com um nível de resistência igual ou superior ao definido para a(s) respetiva(s) porta(s) ou com soluções de segurança composta por vários tipos de materiais que em conjunto asseguram a adequada resistência às ações de intrusão;
 - (2) Porta(s) de acesso ao nível: O número de portas que permitam o acesso à área deste nível devem reduzido ao mínimo indispensável, é recomendado um único ponto de acesso ao local, se houver mais, devem ter as mesmas características de resistência e encontrarem-se bloqueadas pelo interior ou funcionarem somente como portas de evacuação da área em situações de emergência declarada. Deve ser instalada uma porta de segurança de categoria RC3 de acordo com a Norma EN 1627, com ombreira em aço e dobradiças do mesmo material, fixas no lado interior da área;
 - (3) Fechadura da porta de acesso: Deve ser de segurança acionável eletronicamente, resistente a adulterações, de construção em aço inoxidável de alta resistência ou material equivalente (de acordo com a Norma EN 12209 e cilindro de alta segurança de acordo com a Norma EN 1303), reforçada com

uma fechadura eletromagnética(eletoíman), e dispositivo de antipânico. O sistema de abertura elétrico deve ter um nível mínimo de resistência de 300 kg-f, e, utilizar a função “Fail Secure” (Função que bloqueia a porta quando a energia é removida, ou seja, a energia é aplicada para abrir a porta). No lado interior da área de Nível de segurança 3 deverá existir um dispositivo de antipânico que permita desabilitar o sistema em qualquer situação de emergência.

c) Sistema Complementar de Segurança:

(1) Subsistema de Controlo de Acessos (SCA)

- (a) O procedimento de entrada e saída nesta área requer a utilização de mecanismos de identificação baseada, no mínimo em dois fatores de autenticação (p.e.: cartão de proximidade e/ou introdução de PIN-Code e/ou leitura de dados biométricos);
- (b) A porta de acesso a esta área só deverá permitir a entrada e saída através do acionamento de trincos, que funcione de forma automática e após identificação positiva fornecida pelo SCA;
- (c) A porta deverá estar dotada de mecanismos que a obrigue a fechar automaticamente (p.e.: molas de pressão);
- (d) No lado interior da área de Nível de segurança 3 deverá existir um dispositivo de antipânico que permita desabilitar o sistema das portas em qualquer situação de emergência declarada;
- (e) Associado aos sistemas antipânico, existirá sempre um alarme de utilização e um selo de segurança nas restantes portas de acesso do local (que se encontram bloqueadas ou preparadas para qualquer situação de emergência), cujo Encarregado de Segurança substituirá sempre que este método for utilizado, fazendo posteriormente um registo da ocorrência.

(2) Subsistema de Detecção de Intrusão (SDI)

- (a) A área deverá estar equipada com sensores detetores de movimento e sensores magnéticos de abertura;
- (b) O SDI deverá acionar um alarme caso seja detetado algum movimento fora dos períodos normais de atividade, este género de funcionamento, poderá implicar uma programação do sistema para adequar o de calendário de trabalho;
- (c) O SDI deverá acionar um alarme sempre que a porta esteja aberta por um período superior a 20 segundos ou outro tempo que se julgue como necessário para concluir o acesso ao local;
- (d) As janelas, se existirem, devem estar protegidas por um gradeamento de segurança, composto por barras de aço verticais (com 20 mm de diâmetro), distarem entre si cerca de 15 cm e serem suportadas por placas de aço horizontais (com 45 x 6mm) e espaçadas entre 20 cm umas das outras. O gradeamento deve estar solidamente fixo à estrutura do edifício ou à estrutura interna da janela. Devem possuir ainda equipamentos de ocultação ou redução da visibilidade para o interior, podendo ser utilizadas soluções do tipo portadas, estores, cortinados ou aplicação de filtros/películas nos vidros que garantam o ofuscamento necessário em quaisquer condições de funcionamento do serviço.

(3) Subsistema de Videovigilância (SVV)

Esta área deverá estar munida de uma câmara de videovigilância direcionada para a porta de acesso ao nível seguinte (Nível 4), devendo ser colocada de tal forma, que não seja possível visualizar o interior da zona e a captação de imagens com os detalhes de autenticação;

(4) Subsistema Automático de Detecção de Incêndios (SADI)

A área deverá estar equipada com os detetores de incêndios necessários para cobrir a totalidade da área, possuir dispositivos de alarme instalados nas proximidades dos acessos e replicados para o local de monitorização do SCS.

4) Nível de segurança 4

- a) Este nível, constitui-se como o quarto perímetro de segurança. Materializado pela área onde se realizam as atividades da EC, ou seja, a sua zona operacional.
- b) O acesso a esta área apenas é permitido aos funcionários da Organização que formalmente tenham sido designados para exercer funções orgânicas na estrutura da EC.
- c) A permanência nesta área só é possível com a presença de duas pessoas em simultâneo (*Two Men Rule*).
- d) O acesso a esta área só é permitido a elementos pertencentes a grupos distintos na estrutura de pessoal (p.e.: Administrador de Segurança + Operador de Sistemas).
- e) Neste nível, para controlo dos visitantes formalmente autorizados, deverá existir no local um livro para efetuar os registos de acesso. Em alternativa, os visitantes poderão ser controlados por via do SCA, para controlo e registo de todos os acessos efetuados, este procedimento deverá assegurar a sua auditabilidade.
- f) No registo dos visitantes deverá constar: o ano; o mês; o dia; a hora; os minutos de entrada e de saída do local; mais o motivo justificativo da visita e assinatura ou rubrica.
- g) Todo o pessoal da Organização que não exerça funções orgânicas na estrutura da EC tem tratamento igual ao descrito para os visitantes.
- h) Se a área se situar em local propenso a inundações, o local deverá estar equipado com sensores de inundação, para além de a porta e demais equipamentos que permitem o acesso ao interior do local, garantirem a estanquicidade.
- i) Características e tipo de construção da área:
 - (1) Paredes do perímetro exterior desta área devem constituídas por materiais com um nível de resistência a ações de intrusão igual ou superior ao definido para a(s) respetiva(s) porta(s);
 - (2) Teto e pavimento deverá ter uma resistência física estrutural a ações de intrusão igual ou superior à das paredes e porta;
 - (3) O local deve primar pela inexistência de janelas;
 - (4) Porta de acesso ao local: O número de porta que permitam o acesso à área deste Nível devem reduzido ao mínimo indispensável, recomendado um único ponto de acesso ao local, se houver mais devem ter as mesmas características de resistência e encontrarem-se bloqueadas pelo interior ou funcionarem somente como portas de evacuação da área em situação de emergência

declarada. Deve ter instalada uma porta de segurança de categoria RC4 de acordo com a Norma EN 1627 ou normativo similar, com ombreira em aço e dobradiças do mesmo material, fixas no lado interior da área. Fechadura de segurança deve ser resistente a adulterações, ser de construção em aço inoxidável de alta resistência ou material equivalente (de acordo com a Norma EN 12209 e cilindro de alta segurança de acordo com a Norma EN 1303) reforçada com uma fechadura eletromagnética (eletroímã), e dispositivo de antipânico. O sistema de abertura elétrica deve ter um nível mínimo de resistência de 500 kg-f, e, utilizar a função “Fail Secure” (Função que bloqueia a porta quando a energia é removida, ou seja, a energia é aplicada para abrir a porta).

- (5) A porta de acesso ao local deverá estar provida de mecanismo que a obrigue a fechar automaticamente (por exemplo: molas de pressão);
- (6) No lado interior da área de Nível de segurança 4 deverá existir um dispositivo antipânico, que permita desabilitar o sistema de segurança da porta em qualquer situação de emergência declarada;
- (7) Associado aos sistemas antipânico, existirá sempre um alarme de utilização e um selo de segurança nas restantes portas de acesso (que se encontram bloqueadas ou preparadas para qualquer situação de emergência), cujo Encarregado de Segurança substituirá sempre que este sistema for utilizado, fazendo um registo da quebra daquele.

j) Subsistema de Controlo de Acessos (SCA)

- (1) O procedimento de entrada e saída nesta área requer a utilização de mecanismos de identificação apoiada no mínimo em 02 (dois) fatores de autenticação (p.e.: cartão de proximidade e/ou introdução de PIN-Code e/ou leitura de dados biométricos);
- (2) À entrada, um dos fatores de autenticação do acesso deverá recorrer à tecnologia baseada em dados biométricos, configurada de forma a reduzir ao máximo a taxa de aceitação de identificação falsa (FAR - *False Acceptation Rate*);
- (3) À saída deverá existir um leitor de autenticação simples para registo;
- (4) Configuração da porta de acesso:
 - (a) A porta de acesso a esta área só deverá permitir a entrada e saída através do acionamento de trincos que funcionem de forma automática, após a identificação positiva;
 - (b) Deverá ser garantido que a abertura desta porta só é efetuada quando a porta de acesso do nível anterior estiver fechada;
 - (c) Deverá ser garantido que a abertura desta porta (Nível de segurança 4) só é acionada se previamente houver autenticação positiva dos dois intervenientes no acesso do nível anterior.

k) Subsistema de Detecção de Intrusão (SDI)

- (1) A área deverá estar equipada com sensores de deteção de movimento e sensores de contato magnéticos na porta (para verificação de abertura da porta aberta);
- (2) O SDI deverá acionar um alarme sempre que seja detetado algum movimento fora dos períodos normais de atividade;
- (3) O sistema deverá lançar um alarme sempre que a porta esteja aberta por um período superior a 20 segundos ou outro tempo que se julgue como

necessário para concluir o acesso ao local.

l) Subsistema Automático de Detecção e Extinção de Incêndios (SADEI)

- (1) A área deverá estar equipada com um sistema de detecção e extinção automática de incêndios;
 - (2) O elemento extintor deverá permitir poder ser utilizado de forma segura em zonas ocupadas por pessoas, garantindo que é inócuo para os humanos.
- m) Os sistemas de energia que dão suporte ao equipamento que realiza as operações da EC, deverão dispor de fonte de energia alternativa;
- n) A área deverá estar equipada com um sistema de AC independente, devendo estar programado automaticamente para disponibilizar temperaturas de 23°C e humidade relativa de 50%. Todas as condutas e passagens devem estar protegidas com gradeamento ou grelha de segurança que impeça a passagem de pessoas ou equipamentos.

5) Nível de segurança 5

- a) Este nível é materializado pelo Cofre de Segurança onde se encontram os dispositivos (p.e: *Smartcards* de Administradores/Operadores da EC) para acesso ao sistema de gestão do ciclo de vida dos certificados eletrónicos;
- b) O cofre de segurança fica situado no interior da área onde se realizam as atividades da EC (Nível 4);
- c) Todos os indivíduos autorizados e com funções estabelecidas na orgânica da EC com acesso aos sistemas de certificação, deverão ter acesso a este nível;
- d) O Cofre de Segurança deve estar homologado segundo a norma EN 1143-1 para proteção de ações de arrombamento, e a norma EN 1047-1 S 60 DIS para proteção de suportes e dados digitais contra incêndios/fogo.

6) Nível de segurança 6

- a) Este nível é materializado por compartimentos individualizados dentro do cofre, onde se encontram os dispositivos para acesso às funcionalidades do sistema da EC, sendo aconselhável prever a sua abertura por duas pessoas (uma possui o código de abertura e a outra a chave);
- b) Deverá constar um compartimento por cada indivíduo autorizado e com funções estabelecidas na orgânica da EC, ao qual apenas o próprio poderá ter acesso, cujas chaves/fechaduras deverão ter requisitos de segurança, em termos inviolabilidade da fechadura e de cópia da chave (não pode ser uma chave que seja facilmente manufaturada).

6. DIVERSOS

- a. Os requisitos mínimos identificados, no que concerne ao SCS, têm como pressuposto a existência de efetivo de segurança em permanência, 24 horas em todos os dias do ano. A não verificação deste pressuposto, obriga à necessidade de estender este sistema a todo o edifício da EC, com recurso a: detetores de incêndio, detetores de intrusão e

câmaras de videovigilância, direcionadas para a entrada de cada porta que forneça acesso ao nível seguinte.

- b. Ainda neste âmbito, o sistema deve proporcionar a capacidade sinalizar de forma remota os eventos de alarme ao responsável pela segurança da EC.
- c. Todas as condutas existentes, sejam de eletricidade, de ar condicionado e da rede informática, devem ser construídas à base de materiais não combustíveis e de forma alguma podem proporcionar pontos de entrada física para o interior das instalações, bem como a introdução de qualquer material sólido.

7. DIVERSOS

ANS - Autoridade Nacional de Segurança

EC - Entidade Certificadora

FAR - False Aception Rate

GNS - Gabinete Nacional de Segurança

SCA - Subsistema de Controlo de Acessos

SADI - Subsistema de Alarme e Deteção de Incêndios

SDI - Subsistema de Deteção de Intrusão

SADEI - Subsistema de Alarme, Deteção e Autoextinção de Incêndios

SCS - Sistema Complementar de Segurança

SVV - Subsistema de Videovigilância

AC - Ar Condicionado

8. ANEXOS

Nada a referir

9. LISTA DE DISTRIBUIÇÃO

Geral