NORMA TÉCNICA – D 02

REQUISITOS MÍNIMOS DE SEGURANÇA FÍSICA DE INSTALAÇÕES DE ENTIDADES CERTIFICADORAS

Lisboa, 01 de Setembro de 2008

A Autoridade Nacional de Segurança

(José Torres Sobral)

1. REFERENCIAS

Nada a referir

2. SITUAÇÃO

As infra-estruturas de chaves públicas fundamentam, em grande parte, a sua segurança em modelos de confiança baseados em estruturas hierárquicas, em que as Entidades Certificadoras (EC) são o elemento fundamental.

A muita da credibilidade de um sistema de segurança está relacionada com o grau de protecção da sua instalação física. De uma forma geral, se um servidor não está instalado num ambiente seguro, toda a infra-estrutura pode ser comprometida. Levando em conta esta premissa, a actividade operacional de uma EC transcende a simples implementação de um pacote de software e hardware, daí que a segurança do ambiente onde as EC's disponibilizam os seus serviços, deverá ser alvo de particular atenção e estar assente num projecto abrangente, materializando a integração de medidas de segurança física, electrónica, de pessoal e administrativas.

3. OBJECTO/FINALIDADE

A presente norma está relacionada com os aspectos que incidem com a segurança física das instalações onde operam as EC, de modo a assegurar a manutenção da integridade, fiabilidade e confiança dos serviços por estas prestados.

A aplicação destes requisitos mínimos tem em vista a utilização de instalações (p.e.: um edifício) que não são exclusivas da actividade da EC, ou seja, as medidas de segurança mínimas a serem aplicadas ao local e edifício como um todo, de modo a permitir que as actividades das EC se realizem de forma segura.

4. AMBITO

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

5. EXECUÇÃO (Descrição dos níveis de segurança)

Os requisitos descritos nesta norma têm em linha de conta a concepção, construção e localização das Zonas de Alta Segurança (ZAS) e respectivos sistemas, nomeadamente, controlo de acessos, detecção de intrusões, detecção e extinção de incêndios, eléctricos 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, dano, ou interferência. Esta protecção pode ser incrementada (proporcionalmente) sempre que os riscos identificados o justifiquem.

A arquitectura deverá ser formada aplicando o conceito de defesa em profundidade, ou seja, por níveis 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 (integrada) de um conjunto de subsistemas, que em conjunto formam um Sistema de Segurança Electrónico Complementar (SSEC), de funcionamento ininterrupto, proporcionando um ambiente altamente seguro.

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

- Subsistema de Controlo de Acessos (sCA);
- Subsistema de Detecção de Intrusão e Alarme (sDIA);
- Subsistema de Vigilância Vídeo em Circuito Fechado de TV (sVVCFTV);
- Subsistema de Detecção de Incêndios (sDI)
- Subsistema Extinção Automática de Incêndios (sEAI);

Os vários subsistemas devem possuir a máxima integração que a tecnologia possibilite, devendo ser o objectivo final que o SSEC se comporte como um único sistema.

A figura seguinte apresenta uma representação gráfica do ambiente global pretendido, pelo que neste particular, a figura é representativa de uma planta de um edifício situado num local não acessível de forma directa a um possível intruso (p.e.: 2.º piso), quer por meios humanos (p.e.: entrada furtiva), quer por meios físicos (p.e.: arrombamento através de viatura pesada, rebentamento com explosivos.)

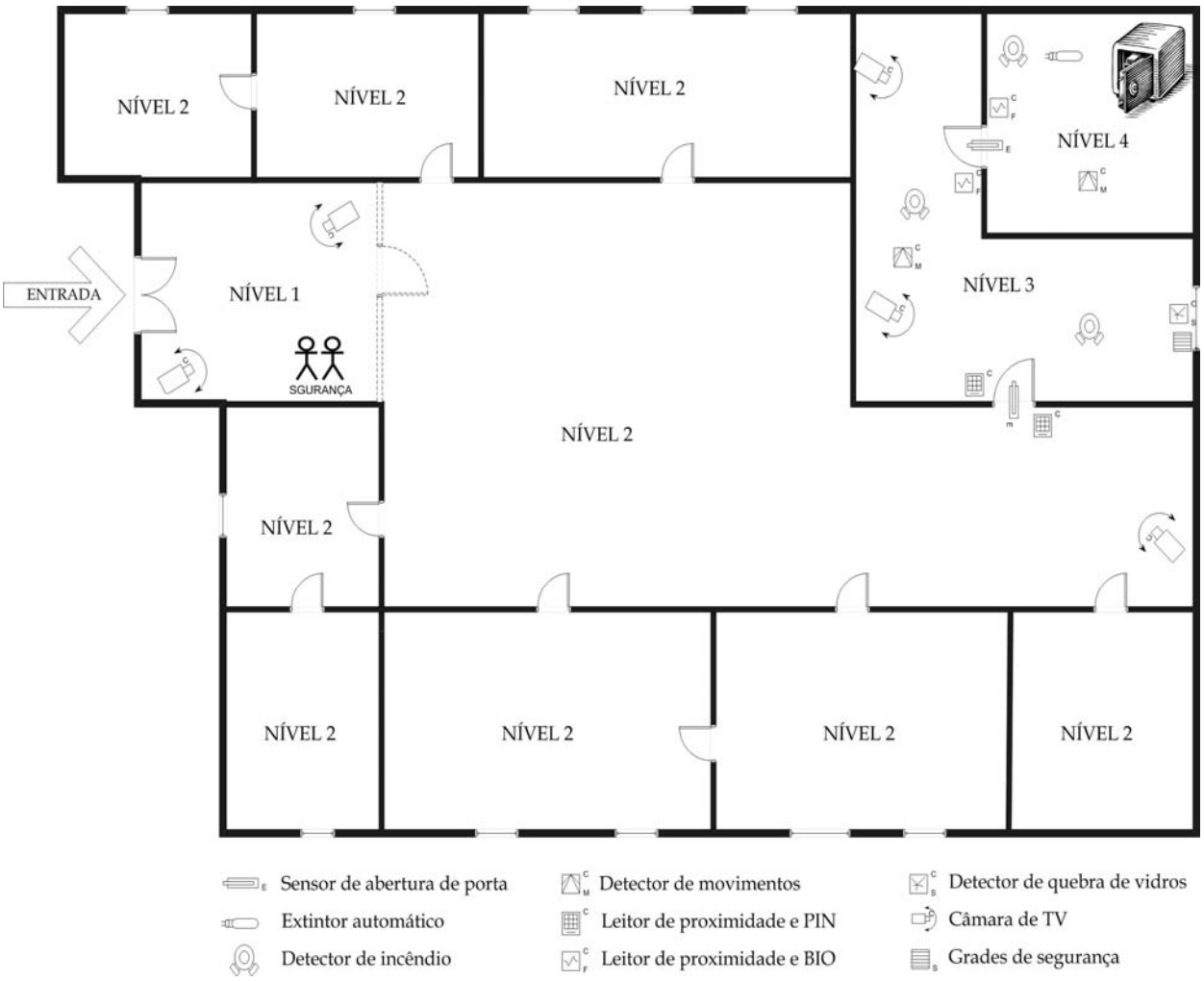

Figura 1 – Ambiente global de segurança

De seguida apresentam-se as características a que deverão obedecer as diferentes camadas 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.

a. NÍVEL 1

1) Este nível constitui-se como o primeiro perímetro de segurança, materializa-se pela entrada e zona de recepção no edifício.
2) É requerido a utilização de um sistema de passes.
3) Pessoal afecto à Organização está sujeito às medidas em vigor para acesso às instalações.
4) Os visitantes são alvo de registo apropriado pelos guardas/seguranças para acesso às instalações.
5) Sistema de Segurança Electrónico Complementar:
    a) Subsistema de Vigilância Vídeo em Circuito Fechado de TV:
        (1) Esta zona deverá estar munida de câmaras de TV, capazes de monitorizar as entradas e saídas em todos os pontos de acesso ao edifício.

b. NÍVEL 2

1) Este nível constitui-se como o segundo perímetro de segurança, é materializado pela zona de trabalho global do organismo/organização (p.e.: zona das salas de trabalho).
2) A circulação dentro deste nível é permitida ao pessoal afecto à organização, de acordo com a metodologia de identificação utilizada no nível anterior.
3) A circulação de visitantes dentro desta área, requer a existência de escolta (guardas ou funcionário visitado).

(Verso em branco)

c. NÍVEL 3

1) Este nível é materializado por ser uma zona de antecâmara para as instalações da EC, pelo que;

2) É uma zona de acesso restrito, servindo de zona tampão de acesso ao nível superior;

3) Esta área garante que o pessoal que circula na zona de trabalho (nível 2), não circule nas imediações da entrada que possibilita o acesso ao nível 4.

4) O acesso a esta área apenas é permitido a pessoal com autorização expressa permanente decorrente das suas funções na estrutura (incluindo serviços de suporte/ apoio) da EC.

5) Os visitantes circulam dentro desta área, apenas sob acompanhamento de escolta (funcionário autorizado ou guardas).

6) Características e tipo de construção da área:

   a) Paredes em alvenaria, betão ou tijolo ou material equivalente;

   b) Porta de segurança, com chapa em aço, com as dobradiças fixas no lado interior de ombreira igualmente em aço, fechadura de segurança accionável electronicamente e características antipânico.

7) Sistema de Segurança Electrónico Complementar:

   a) Subsistema de Controlo de Acessos (sCA):

      (1) O procedimento de entrada e saída nesta área requer a utilização de mecanismos de identificação baseada em dois factores (p.e.: cartão de proximidade + PIN);

      (2) A porta de acesso a esta área só deverá permitir a entrada e saída através do accionamento de trincos que funcionem de forma automática e após identificação positiva fornecida pelo sCA.

      (3) As portas deverão estar dotadas de mecanismos a obriguem a fechar automaticamente (p.e.: molas de pressão).

      (4) As portas deverão, disponibilizar um meio manual de abertura, apenas a partir do seu interior, a ser utilizado exclusivamente em eventos de pânico.

(Verso em branco)

b) Subsistema de Detecção de Intrusão e Alarme (sDIA):

(1) A área deverá estar equipada com detectores de movimento e sensores de porta aberta/fechada.

(2) O sDIA deverá lançar um alarme sempre que seja detectado algum movimento nos períodos em que o sCA tenha informação da não existência de actividade no interior da área.

(3) O sDIA deverá lançar um alarme sempre que a porta esteja aberta por um período superior a 20 segundos.

(4) As janelas (se houver) devem ser protegidas por material opaco e estar dotadas de barras de aço embebidas, pelo menos 2 cm na estrutura da parede, distanciando entre si não mais de 15 cm, sendo obrigatório a existência de detectores de quebra de vidro.

c) Subsistema de Vigilância Vídeo em Circuito Fechado de TV:

(1) Esta área deverá estar munida com pelo menos duas câmaras de TV, uma direccionada para a porta do nível respectivo, a outra direccionada para a porta do nível seguinte.

(2) A câmara de TV direccionada para a porta do nível seguinte (Nível 4), deverá ser colocada de tal forma, que nunca seja possível visualizar o interior da zona.

d) Subsistema de Detecção de Incêndios:

(1) A área deverá estar equipada com os detectores de incêndios necessários, tendo em conta a dimensão da área.

d. NÍVEL 4

1) Este nível, constitui-se como o quarto perímetro de segurança, é materializado pela área onde se realizam as actividades da EC, ou seja, a zona operacional da Entidade Certificadora

2) O acesso a esta área apenas é permitido aos funcionários que formalmente tenham sido designados para exercer funções orgânicas na estrutura da EC.

3) O acesso a esta área só é permitido com duas pessoas em simultâneo (Two Men rule);

4) O acesso a esta área só é permitido a elementos pertencentes a grupo distintos na estrutura de pessoal (por exemplo: Administrador de Segurança+Operador de Sistemas);

5) Deve constar no local, um livro de registos (com folhas numeradas) para visitantes.

(Verso em branco)

6) Os visitantes são alvo de registo onde conste: o ano, o mês, o dia, a hora de entrada/saída e o motivo da visita);

7) Todo o pessoal que não exerça funções orgânicas na estrutura da EC tem tratamento igual ao descrito para os visitantes.

8) Se a área se situar em local propenso a inundações, o local deverá estar equipado com sensores de inundação.

9) Características e tipo de construção da área:

   a) Paredes em alvenaria, betão ou tijolo ou material equivalente;

   b) Tecto e pavimento com construção similar à das paredes;

   c) Inexistência de janelas;

   d) Porta de segurança, com chapa em aço em aço, com as dobradiças fixas no lado interior de ombreira igualmente em aço, com de fechadura de segurança accionável electronicamente, características corta – fogo e antipânico.

10) Sistema de Segurança Electrónico Complementar:

   a) Subsistema de Controlo de Acessos:

      (1) O procedimento de entrada e saída nesta área requer a utilização de mecanismos de identificação baseada no mínimo em 2 (dois) factores em que um deles é obrigatoriamente o recurso a tecnologia baseada em biometria (na entrada), em que o leitor deverá estar configurado de forma a reduzir ao máximo a taxa de aceitação de identificação falsa (FAR - False Aception Rate).

      (2) A porta de acesso a esta área só deverá permitir a entrada e saída através do accionamento de trincos que funcionem de forma automática, após identificação positiva fornecida pelo sCA.

      (3) O sCA deverá garantir que a abertura desta porta de acesso só é accionada se a porta de acesso do nível anterior estiver fechada

      (4) O sCA deverá garantir que a abertura desta porta de acesso só é accionada se previamente houver autenticação positiva dos intervenientes no acesso do nível anterior.

      (5) As portas deverão estar dotadas de mecanismos a obriguem a fechar automaticamente.

      (6) As portas deverão, disponibilizar um meio manual de abertura, apenas a partir do seu interior, a ser utilizado exclusivamente em eventos de pânico.

b) Subsistema de Detecção de Intrusão e Alarme:

(1) A área deverá estar equipada com detectores de movimento e sensores de porta (para verificação de porta aberta/fechada).

(2) O sistema deverá lançar um alarme sempre que seja detectado algum movimento nos períodos em que o SCA tenha informação da não existência de actividade no interior da área.

(3) O sistema deverá lançar um alarme sempre que a porta esteja aberta por um período superior a 20 segundos.

c) Subsistema Extinção Automática de Incêndios:

(1) A área deverá estar equipada com um sistema de 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 o homem.

d) Os sistemas de energia que dão suporte ao equipamento que realiza as operações da EC, deverão dispor de fonte de energia alternativa;

e) A área deverá estar equipada com um sistema de AC independente, devendo estar programado para disponibilizar temperaturas de 20ºC e humidade relativa de 50%.

e. NÍVEL *5*

1) 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.

2) O cofre de segurança fica situado no interior da área onde se realizam as actividades da EC.

3) Todos os indivíduos autorizados e com funções estabelecidas na orgânica da EC com acesso aos sistemas de certificação, deverão ter acesso a este nível.

4) O Cofre de Segurança, deve estar homologado segundo a norma EN 1143-1.

f. NÍVEL 6

1) Este nível é materializado por compartimentos individualizados dentro do cofre, onde se encontram os dispositivos para acesso às funcionalidades do sistema da EC.

2) Deverá constar um compartimento por cada indivíduo autorizado e com funções estabelecidas na orgânica da EC, ao qual apenas o próprio poderá ter acesso.

6. DIVERSOS

Os requisitos mínimos identificados, no que concerne ao SSEC, tem como pressuposto a existência de guardas/seguranças em permanência, 24 horas, todos os dias do ano. A não verificação deste pressuposto, obriga à necessidade de estender este sistemas a todo o edifício, nomeadamente, detectores de incêndio, detectores de quebra de vidro, câmaras de TV (direccionadas para a entrada de cada porta que forneça acesso ao nível seguintes) e detectores de movimento.

Ainda neste âmbito o sistema deve proporcionar a capacidade de, de forma remota, sinalizar eventos de alarme ao responsável pela segurança da EC.

Todas as condutas existentes, nomeadamente, eléctricas, de ar condicionado, Rede Informática, devem ser construídas à base 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. ACRÓNIMOS

ANS	Autoridade Nacional de Segurança
FAR	False Aception Rate
GNS	Gabinete Nacional de Segurança
sCA	Subsistema de Controlo de Acessos
sDI	Subsistema de Detecção de Incêndios
sDIA	Subsistema de Detecção de Intrusão e Alarme
sEAI	Subsistema de Extinção Automática de Incêndios
SSEC	Sistema de Segurança Electrónico Complementar
sVVCFTV	Subsistema de vigilância vídeo em circuito fechado de TV
ZAS	Zona de Alta Segurança

8. ANEXOS

Nada a referir

9. DISTRIBUIÇÃO

Permitida a distribuição pela Internet