GNS
Gabinete Nacional de Segurança

NORMA TÉCNICA – D 01

REQUISITOS PARA A CREDENCIAÇÃO DE AUDITOR DE SEGURANÇA, PREVISTAS NO DECRETO REGULAMENTAR Nº 25/2004, DE 15 DE JULHO.

Lisboa, 01 de Junho de 2007

A Autoridade Nacional de Segurança

(José Torres Sobral)

1. REFERÊNCIAS

a. Decreto-Lei nº 170/2007, de 3 de Maio;

b. Decreto-Lei nº 290-D/99, de 2 de Agosto;

c. Decreto Regulamentar nº 25/2004, de 15 de Julho;

d. Norma ISO/IEC 17799.

2. SITUAÇÃO

a. Nos termos do artigo 3º do Decreto-Lei nº 170/2007, de 3 de Maio, a Autoridade Nacional de Segurança (ANS) exerce a autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de matérias classificadas, cabendo-lhe também exercer as competências que lhe são cometidas pelas normas nacionais de segurança em vigor.

b. O Decreto Regulamentar nº 25/2004, de 15 de Julho, que regulamenta o Decreto-Lei nº 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital, envolve a ANS nas credenciações de segurança, sempre que estejam em causa matérias classificadas.

c. Assim, no quadro fixado pelo referido diploma, compete à ANS, designadamente, proceder a avaliações de segurança de entidades certificadoras antes do início da respectiva actividade; aprovar os planos de segurança e de contingência e as políticas de pessoal e credenciar as entidades subcontratadas e os auditores de segurança.

d. Assumindo particular importância a figura do auditor de segurança, atentas, sobretudo, as suas especiais responsabilidades em matéria de segurança de informação, importa fixar as condições necessárias ao exercício de tais funções.

3. OBJECTO/FINALIDADE

A presente norma define os requisitos necessários ao exercício das funções de auditor de segurança, no âmbito do processo de credenciação a que se refere o nº 1 do artigo 30º do Decreto Regulamentar nº 25/2004, de 15 de Julho.

4. ÂMBITO

A presente norma aplica-se a todas as pessoas, singulares e colectivas, que pretendam ser credenciadas como auditor de segurança, nos termos e para os efeitos do disposto no artigo 30° do Decreto Regulamentar n° 25/2004, de 15 de Julho.

5. EXECUÇÃO

As pessoas, singulares ou colectivas, que pretendam exercer as funções de auditor de segurança serão credenciadas pela ANS se preencherem, cumulativamente, as condições previstas no n° 1 do artigo 30° do Decreto Regulamentar n° 25/2004, de 15 de Julho, e os requisitos previstos no ponto seguinte:

a. Requisitos e Competências

Ao auditor de segurança é exigido, obrigatoriamente, a conformidade com os critérios abaixo descritos[1]:

1) Possuir formação académica de nível superior ou sua equiparação mediante valorização de currículo profissional;

2) Ter, no mínimo, quatro anos de experiência de trabalho, a tempo inteiro, em assuntos relacionados com tecnologias de informação, em que pelo menos 2 (dois) desses anos tenham sido desenvolvidos em cargos ou funções relacionadas com segurança da informação;

3) Possuir conhecimentos, no âmbito da segurança da informação, sobre a condução de análises de risco, de forma a identificar os activos, ameaças e vulnerabilidades a que estão sujeitas as Entidades Certificadoras (EC), no sentido de compreender o impacto, consequente minimização e controlo dos riscos;

4) Ter conhecimentos actualizados nos assuntos relacionados com as tecnologias em que se baseiam as Infra-estruturas de Chaves Públicas (ICP), em que tenha exercido funções relacionadas com tecnologia de ICP, pelo menos durante 1 (um) ano;

5) Ter conhecimentos actualizados nos assuntos relacionados com a gestão da segurança da informação e análise e avaliação de sistemas;

6) Ser fiável e possuir qualidades de lealdade funcional, competência profissional e idoneidade cívica;

---

[1] Os requisitos referidos nas alíneas 9), 10), 11) e 12) são detidos por um único indivíduo, o coordenador de equipa de auditoria.

7) Ter capacidade para detectar e analisar incidentes de segurança nos registos das operações realizadas pela EC durante a sua actividade;

8) Conhecer, compreender e interpretar de forma adequada os princípios e processos relativos à análise, avaliação e gestão do risco;

9) Estar apto para a preparação, distribuição de tarefas e condução de equipas de auditoria, bem como no âmbito da revisão da documentação e avaliação da auditoria;

10) Possuir experiência na elaboração e apresentação de relatórios finais de auditoria;

11) Ter completado com aproveitamento um curso de formação, com duração mínima de 35 horas, em matérias relativas à auditoria de sistemas de gestão da segurança da informação, nacional ou internacionalmente reconhecido, ou cujo currículo seja aprovado pela ANS;

12) Ter exercido actividade de auditor em pelo menos quatro auditorias de segurança;

13) Conhecer e interpretar a legislação nacional, relativa à assinatura electrónica.

b. O Processo de Candidatura

O processo de candidatura para auditor de segurança será instruído de acordo com as regras e procedimentos internos definidos para a credenciação de segurança.

A formalização da candidatura deverá ser dirigida ao Gabinete Nacional de Segurança da Presidência do Conselho de Ministros.

Dependendo da natureza jurídica do auditor de segurança, "pessoa colectiva" ou "singular", o conjunto de documentação é a que a seguir se discrimina:

1) Pessoa Colectiva

Ofício em papel timbrado da empresa, dirigido ao Gabinete Nacional de Segurança da Presidência do Conselho de Ministros, solicitando a CREDENCIAÇÃO EM AUDITOR DE SEGURANÇA DE ENTIDADES CERTIFICADORAS, AO ABRIGO DO DECRETO REGULAMENTAR Nº 25/2004, DE 15 DE JULHO.

Devem ser incluídos como anexos os seguintes documentos:

a) Certidão da Conservatória do Registo Comercial ou fotocópia autenticada;

b) Fotocópia do Cartão de Identificação de Pessoa Colectiva;

c) Fotocópia (s) do (s) Diário (s) da República, III Série, que publicaram os estatutos da empresa e suas posteriores alterações, nomeadamente o objecto social;

d) Alvará (fotocópia), se a actividade assim o exigir;

e) Currículo da pessoa colectiva (trabalhos realizados que entender evidenciar em seu abono);

f) Declaração, referindo o cumprimento do disposto no nº 4 do artigo 30º do Decreto Regulamentar nº 25/2004;

g) Individualmente, por cada membro da equipa de auditoria, deverão ser entregues os seguintes elementos:

(1) Uma fotografia a cores;

(2) Certificado de Registo Criminal para efeitos de credenciação em auditor de segurança de Entidades Certificadoras;

(3) Fotocópia do Bilhete de Identidade;

(4) Declaração, garantindo que o candidato é fiável e possui qualidades de lealdade funcional e idoneidade cívica para exercer as funções de auditor de segurança, assinada pela entidade máxima da empresa;

(5) Currículo detalhado;

(6) Outros elementos e/ou referências considerados relevantes para a demonstração da aptidão para o exercício da função de auditor de segurança.

h) Ao membro da equipa que desempenhe a função de auditor coordenador, é requerido adicionalmente, a apresentação de:

(1) Documentos comprovativos do exercício da actividade de auditor (ver 6.a., onde conste, para cada uma das auditorias:

- A identificação da entidade auditada;
- A identificação do auditor;
- A data, duração e âmbito da auditoria.

(2) Original do certificado do respectivo curso de formação referido em 5.a.11).

2) Pessoa Singular

Ofício dirigido ao Gabinete Nacional de Segurança da Presidência do Conselho de Ministros, solicitando a CREDENCIAÇÃO EM AUDITOR DE SEGURANÇA DE ENTIDADES CERTIFICADORAS, AO ABRIGO DO DECRETO REGULAMENTAR Nº 25/2004, DE 15 DE JULHO.

Devem ser incluídos como anexos os seguintes documentos:

a) Declaração, referindo o cumprimento do disposto no nº 4 do artigo 30º do Decreto Regulamentar nº 25/2004;

b) Uma fotografia a cores;

c) Certificado de Registo Criminal para efeitos de credenciação em auditor de segurança de Entidades Certificadoras;

d) Fotocópia do Bilhete de Identidade;

e) Fotocópia do Cartão de Contribuinte;

f) Carta de referência pessoal, atestando que o candidato é fiável e possui qualidades de lealdade funcional e idoneidade cívica para exercer as funções de auditor de segurança;

g) Carta de referência de entidade empregadora, na qual preste ou já tenha prestado serviço, atestando que o candidato é fiável e possui qualidades de lealdade funcional e idoneidade cívica para exercer as funções de auditor de segurança;

h) Original do certificado do respectivo curso de formação referido em 5.a.11);

i) Currículo detalhado;

j) Documentos comprovativos do exercício da actividade de auditor (ver 6.a.), onde conste, para cada uma das auditorias:

- A identificação da entidade auditada;
- A identificação do auditor;
- A data, duração e âmbito da auditoria.

k) Outros elementos e/ou referências considerados relevantes para a demonstração da aptidão para o exercício da função de auditor de segurança.

6. DIVERSOS

a. Conceitos e Definições

Os conceitos descritos nesta norma apenas dizem respeito à mesma e têm como objectivo auxiliar a sua interpretação.

- **Auditor de Segurança**: é uma pessoa singular ou colectiva, independente da entidade certificadora, de reconhecida idoneidade, experiência e qualificações comprovadas na área da segurança de informação, na execução de auditorias de segurança e na utilização da norma ISO/IEC 17799, devidamente credenciada pela Autoridade Nacional de Segurança.

b. Considera-se documentação adequada para comprovação da actividade de auditor, entre outros, declarações da(s) entidade(s) que foram alvo das auditorias, os Relatórios de Auditoria ou outra à consideração do avaliado desde que permita aferir a validade das auditorias;

c. Todas as referências e elementos incluídos nos Curricula deverão ser acompanhados dos respectivos comprovativos;

d. A ANS pode ainda convocar o candidato para uma entrevista pessoal com carácter supletivo;

e. Serão aceites apenas os processos que reunam os requisitos mínimos de candidatura constantes neste documento, os quais serão devidamente comprovados;

f. Efectuada a análise do processo, os candidatos são informados da sua aceitação ou recusa no prazo de 30 (trinta) dias, a contar da data de entrega de toda a documentação requerida;

g. A credenciação concedida pela ANS tem validade por um período de 3 (três) anos;

h. Sempre que haja na estrutura do auditor de segurança alterações relevantes que possam constituir alteração aos requisitos e elementos que serviram de base à atribuição da credenciação, o auditor de segurança é obrigado a comunicá-los à ANS, no prazo de 15 dias úteis contados da data da sua verificação.

7. ACRÓNIMOS

ANS – Autoridade Nacional de Segurança

EC – Entidade Certificadora

GNS – Gabinete Nacional de Segurança

ICP – Infra-estrutura de Chaves Públicas

8. ANEXOS

Nada a referir.