Audição na AR perante a Comissão do Orçamento, Finanças a AP
02 JUN – 17H00

Discurso de introdução aos deputados sobre a ANS

Tópicos

- A Autoridade Nacional de Segurança O.T.A.N foi criada no final dos anos 50 decorrente da nossa adesão à NATO, com base num acordo datado de 04 de abril de 1949 entre a NATO e os Países fundadores.
- Desde 1997 (Dec-Lei 217/97, 20Agosto) está integrada na PCM dependendo do PM.
- Entre os finais dos Anos 80 até 1994 foram publicados os Segnac's 1 a 4 (RCMs) que contêm as normas nacionais para protecção de um modo geral, a tudo o que se refere a matéria classificada. Até essa altura a actividade era regulada pelas normas NATO.
- **SEGNAC 1** - RCM 50/88, 03Dez alterada pela RCM 13/93, 06Mar – Segurança da Informação Classificada
- **SEGNAC 2** - RCM 37/89, 24Out – Segurança Industrial, Tecnológica e de Investigação
- **SEGNAC 3** - RCM 16/94, 22Mar – Segurança das Telecomunicações
- **SEGNAC 4** - RCM 5/90, 28Fev – Segurança dos Sistemas de Informação
- Os Segnac's publicados na forma de RCM, foram, ao longo de 20 anos ficando desactualizados, em resultado das publicações de diversas leis como as do segredo de Justiça, segredo de Estado, Profissional etc.
  Ao longo desse período as directivas comunitárias e sobretudo as da NATO trouxeram uma grande variedade de novas normas em publicações de diversos formatos.

Na impossibilidade de actualizarmos os Segnac's optou a ANS pela publicação de normas técnicas introduzindo nova doutrina. Essas NT são na sua maioria editadas em publicações do GNS e colocadas no site respectivo.

- A ANS no decorrer da sua vida esteve Tutelada inicialmente pelo PM (Conselho de Ministros) e entre 1982 e 1997 pelo MDN, voltando novamente à tutela do PM até ao presente. Através de diversas LO foram-lhe atribuídas mais funções, nomeadamente novas missões e atribuições, como a inclusão da AND, encarregada de produzir, distribuir e controlar todas as cifras usadas no País. Em 1997 e sob a tutela do PM, estendeu as suas responsabilidades à segurança das matérias classificadas nacionais e de outros parceiros ao abrigo de acordos internacionais como os da EU.
- Nos últimos dez anos a segurança da informação evoluiu muito depressa e em poucos anos a ANS foi alvo de outras LO que acrescentaram responsabilidades no campo da credenciação das unidades certificadoras de assinatura electrónica e da estrutura da SCEE.
- A principal preocupação neste período foi assegurar a formação adequada dos seus quadros que estavam distribuídos por 8 equipas multidisciplinares com missões bem definidas.
- Assim e de parceria com o CEGER assegurou-se a formação de técnicos qualificados em Tecnologias de Informação e Comunicações (TIC) normas ISO entre outros cursos de longa duração com universidades nacionais e estrangeiras. Foi com eles que se trabalhou na elaboração do estudo ENSI trabalho muito completo e actual que foi entregue em 2004, e sob a direcção da UMIC dirigida pelo Dr. Diogo Vasconcelos, que infelizmente não se conseguiu dar andamento às propostas.
- Entretanto em cooperação com a nossa congénere israelita prepararam-se cursos de segurança industrial e de segurança de matérias classificadas onde se colocou a doutrina da NATO e a experiência dos israelitas.

- Mais tarde, em 2011, voltou-se à questão da cibersegurança que preocupava muito os decisores políticos. Foi criada uma CI que produziu um extenso e completo relatório. Em 2014 com uma nova LO (DL 69/2014 de 09maio) foi criado o Centro Nacional de Cibersegurança (CNCS), sob jurisdição da ANS e é com gosto que lhes posso afirmar que no tocante à maior prioridade – a detecção de ataques já se atingiu a capacidade operacional.
- Em 2010 houve ainda uma nova LO que atribuiu ao GNS a capacidade de cobrar taxas para retribuição de diversas actividades, conjugadas numa portaria. Deste modo o GNS nos anos seguintes assegurou uma estabilidade financeira cujas despesas são cobertas pelas receitas em cerca de (85%).
- A presente lei fixa os princípios e as regras gerais, os requisitos e as condições a que as plataformas electrónicas devem obedecer, sendo ainda estabelecidas as obrigações e as condições de interoperabilidade das mesmas entre si, bem como com o Portal dos Contratos Públicos e com outros sistemas de entidades públicas.
- A presente lei estabelece ainda as regras, os requisitos e as especificações técnicas a que as comunicações e as trocas de dados e de informações processados através de plataformas electrónicas nos termos estabelecidos no CCP, devem obedecer.
- O modelo agora proposto visa criar um novo modelo de *governance*, baseado numa entidade supervisora deste mercado, o Instituto dos Mercados Públicos, do Imobiliário e da Construção, I.P., atendendo às competências que detém em matéria de contratos públicos e é a entidade que deve assegurar o licenciamento, a monitorização e a fiscalização das plataformas electrónicas de contratação pública.
- Por outro lado, o quadro legal a implementar exige ainda a existência de uma entidade credenciadora, que atendendo à elevada complexidade e tecnicidade desta atividade de credenciação e pela especial aptidão que esta entidade possui para atuar como Autoridade Credenciadora (AC), bem como pelo fato de

se encontrar integrada na Presidência do Conselho de Ministros e garantir forte hierarquia de segurança, foi entendido que deve ser o Gabinete Nacional de Segurança a entidade competente para assegurar a credenciação das plataformas electrónicas.

- Os contributos do GNS para a elaboração desta proposta de lei, basearam-se nos seguintes fundamentos:
- Diretamente, através das atuais atribuições do GNS, enquanto entidade supervisora e credenciadora, para os assuntos relacionados com a certificação electrónica, no domínio púbico (Sistema de Certificação Electrónico De Estado - SCEE) e domínio privado (âmbito do decreto-lei 290-D/99) e no âmbito da iniciativa de cidadania europeia, enquanto Autoridade Nacional para a Certificação dos Sistemas de Recolha de declarações por Via Electrónica (SRVE). A iniciativa de cidadania europeia, permite que um milhão de cidadãos da União Europeia de, pelo menos, sete países da União convidem a Comissão Europeia a apresentar propostas legislativas em domínios em que a UE tem competência para legislar. Estes registos são feitos em sistema electrónico *online* e as regras e os procedimentos que regem a iniciativa de cidadania estão definidos num regulamento da UE adotado pelo Parlamento Europeu e pelo Conselho da União Europeia em Fevereiro de 2011).
- Dado o anterior enquadramento importa agora materializar e enquadrar de forma genérica as opções tomadas na letra da lei no que diz respeito à segurança das plataformas e dos dados por estas processadas.
- O Modelo de gestão de Tecnologia de Informação e de gestão de segurança é baseado nos standards mais reconhecidos pela indústria, nomeadamente, a família das ISO/IEC 20000 e 27000. Neste particular, houve especial atenção, em não onerar as entidades gestoras das plataformas, com a necessidade de obter a certificação nas normas, mas apenas a obrigatoriedade da sua implementação.
- O modelo de supervisão das auditorias de segurança, seguido pelo GNS, é baseado nas recomendações europeias, que incentivam

para que sejam os *players* do mercado com competências a realizar este tipo de auditorias de segurança.

- Este é o modelo em vigor no GNS para os prestadores de serviços de certificação electrónica e que agora é posto em prática nesta proposta de lei.
- Resumidamente, a autoridade (o GNS) define os requisitos e competências dos auditores de segurança (materializada na nossa norma técnica D-01 e disponível no nosso website), e são os potenciais auditores de segurança (pessoas colectivas ou singulares) que se podem submeter a um processo de credenciação para conseguirem tal habilitação. Ainda neste âmbito, o GNS, relaciona-se estreitamente como os auditores de segurança e tem sempre a última palavra na decisão sobre a auditoria.
- Atualmente os auditores que realizam as auditorias às Plataformas Electrónicas são credenciados pelo GNS e estão numa lista publicada no website do GNS.
- O GNS disponibiliza um conjunto alargado de normas que enquadram as atividades referidas anteriormente, nomeadamente:
- GNS / NT-D 01 - Requisitos para a Credenciação de Auditor de Segurança previstos no Decreto Regulamentar nº 25/2004, de 15 de Julho
- GNS / NT-D 02 - Requisitos mínimos de Segurança Física de Instalações de Entidades Certificadoras
- GNS / NT-D 03 - Requisitos para Entidades Certificadoras que emitem Certificados Qualificados
- GNS / NT-D-04 - Regras para a Auditoria de Entidades Certificadoras que emitem Certificados Qualificados
- GNS / NT-D 05 - Norma Técnica sobre as regras para a certificação de SRVE
- Logo que esta proposta de lei entre em vigor o GNS iniciará a mesma política publicando normas, no âmbito das plataformas

electrónicas de contratação pública que ajudem a enquadrar as especificações próprias das actividades dos auditores e auditados.

- Ainda no âmbito da certificação electrónica, estão credenciadas cinco entidades certificadoras públicas e duas privadas. O detalhe destas entidades e serviços de certificação prestados estão descritos em detalhe, no website do GNS, na Trusted-Service Status List, abreviadamente designada por TSL.
- A TSL é baseada numa norma europeia definida para o efeito e é gerida por um entidade própria em cada estado membro (em Portugal é o GNS) e disponibilizada em duas versões:
- - formato PDF (human readable)
- - formato XML (machine readable).
- Considerando que os potenciais candidatos à credenciação, cumprem na generalidade com os requisitos definidos na proposta de lei, o processo de credenciação em regra não excederá os 60 dias.