Contributos em sede de consulta pública

Preparado para:

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Dezembro 2021

Exmo. Sr. subdiretor-geral do Gabinete Nacional de Segurança responsável pela coordenação do Centro Nacional de Cibersegurança

Eng.º Lino Santos

Vimos apresentar os nossos contributos e sugestões relativamente ao projeto de regulamento que configura instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes.

Este documento expressa a nossa posição tendo em conta a conjuntura tecnológica existente à data em que o documento foi submetido.

Na expectativa de podermos contribuir para uma melhoria de maturidade na gestão da cibersegurança em Portugal, estamos disponíveis para os esclarecimentos que julguem convenientes.

Aceite os meus melhores cumprimentos,

Porto, 29 de dezembro de 2021

(contacto: hnecho@necho.pt)

CONTRIBUTOS EM SEDE DE CONSULTA PÚBLICA

DO AVISO N.º 21606/2021 - CNCS[1]

Projeto de regulamento que configura uma Instrução Técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes.

Para uma maior maturidade dos termos de aplicação do normativo que estabeleceu o regime jurídico da segurança do ciberespaço[2] (**RJSC**), propõe-se a densificação de disposições da "Instrução Técnica relativa à comunicação e informação"[3], em consulta pública, sugerindo-se as seguintes alterações:

1. Garantir a autenticidade e integridade da informação transmitida ao CNCS

As comunicações a estabelecer entre as entidades e o CNCS deverão ser efetuadas de modo a:

a) Garantir a autenticidade da entidade emissora;

b) Garantir a integridade da informação transmitida ao CNCS.

1.1 Proposta: Alterar o n.º 2 do art.º 1.º da proposta de Instrução Técnica, de forma a serem garantidos os princípios de autenticidade da entidade emissora e a integridade da informação transmitida.

[1] Centro Nacional de Cibersegurança, https://www.cncs.gov.pt/
[2] Decreto-Lei n.º 65/2021, de 30 de julho, que Regulamenta o Regime Jurídico da Segurança do Ciberespaço
[3] CNCS, Aviso n.º 21606/2021

2. Densificar a informação relativa ao "Ponto de Contato Permanente" e ao "Responsável da Segurança".

A designação obrigatória para determinadas funções já ocorre noutros normativos em vigor. Assim, e face à importância de uma abordagem holística nos processos de conformidade no âmbito da proteção da informação, designadamente no âmbito da cibersegurança e da proteção de dados, sugere-se utilizar um formulário similar ao implementado pela CNPD[4] no âmbito da designação do "encarregado de proteção de dados" para conformidade com o RGPD[5], que está disponível em https://www.cnpd.pt:8086/dpo/

2.1 Proposta: Alterar o ANEXO I e o ANEXO II da proposta de Instrução Técnica de forma a acomodar a seguinte informação:

a) Identificação e contactos da entidade:

- Nome Entidade

- NIF

- Morada (Rua, Nº, Código Postal e Localidade)

- País

b) Identificação e contactos da pessoa designada:

- Nome da pessoa

- País onde se encontra

- Contactos principais (telefone/telemóvel e email)

- Contactos alternativos (telefone/telemóvel e email)

c) Relação de trabalho da pessoa designada com a entidade:

- Relação de trabalho com a entidade: (interna/externa)

  - Se externo, a entidade notificadora tem: (contrato com a organização/outro)

- A quem é que a pessoa reporta dentro da organização: (Administração/Direção/etc..)

[4] Comissão Nacional de Proteção de Dados, https://www.cnpd.pt/
[5] Regulamento Geral sobre a Proteção de Dados, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

- Qual é o regime de trabalho: (Tempo inteiro/Tempo parcial)

- Ele/ela tem outras funções dentro da organização: (Não/Sim)

  - Se tem, que tipo?

- Data de início das funções

- Onde está inserida a pessoa no organigrama da organização: (Administração/Direção/etc..)

3. Densificar a classificação dos ativos[6]

Na segurança da informação, a gestão de ativos é uma atividade fundamental sem a qual várias outras atividades não poderiam ser eficazmente geridas, designadamente, a gestão de vulnerabilidades e do risco, a gestão de incidentes, a gestão da segurança dos dados, etc.

Assim, e bem, na regulamentação do RJSC está previsto que "*as entidades devem elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços*"[7]. Já no âmbito da proposta de Instrução Técnica sob consulta pública estabelece-se que a informação a constar do inventário de ativos deve ser baseada nas medidas técnicas «ID.GA — Gestão de Ativos», do Quadro Nacional de Referência de Cibersegurança (QNRCS), elaborado pelo CNCS e publicado no respetivo sítio na Internet.

Ora, uma organização implementa controlos para assegurar que os seus objetivos organizacionais sejam atingidos, os riscos sejam reduzidos e os erros sejam prevenidos ou corrigidos. Tipicamente, os controlos são utilizados de duas formas: são criados para assegurar resultados desejados ou são criados para evitar resultados indesejados.

No caso, os controlos da classe ID.GA têm como objetivo assegurar que a organização identifica os dados, colaboradores, equipamentos, sistemas e instalações que permitem atingir os seus objetivos organizacionais. Os controlos desta classe têm também como objetivo garantir que esses ativos, agora inventariados, são geridos de forma consistente com a sua importância relativa para com os objetivos organizacionais e para com a

[6] "*...entende-se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerandos essenciais, que suportam, direta ou indiretamente, um ou mais serviços*" (n.º 1 do art.º 4º do projeto de instrução técnica)
[7] N.º 1 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021

estratégia de risco da organização. Entre outras medidas técnicas, é requerido que os ativos sejam classificados de acordo com a sua criticidade para a organização.

3.1 Proposta: Face ao exposto, parece-nos pertinente que sejam densificados os termos de classificação destes ativos (essenciais para a prestação dos respetivos serviços), incorporando elementos sobre:

a) Informação sobre os ativos:

- Categoria do ativo (ex: Hardware, Software, Rede de Comunicações, Dispositivo IT, Ativo Virtual, Informação, Pessoal, Registos, etc..)

- Valorização do ativo (ex: custo da sua substituição por perda total)

- Localização geográfica do ativo (país)

- Proprietário do ativo (Organização/Fornecedor externo/etc..)

b) Detalhes técnicos:

- N.º de Inventário

- N.º de Série

c) Análise Prévia de Risco:

- Volume de informação

- Tipo de informação (ex: Processos de negócio, Dados organizacionais, Dados pessoais, Dados Sensíveis, Dados Anonimizados, etc...)

d) Dimensões de segurança:

- Confidencialidade, medidas em vigor para evitar o acesso inadequado aos dados (ex: divulgação a pessoas não autorizadas ou a pessoas que não têm necessidade de conhecer a informação)

- Integridade, medidas em vigor para prevenir ou impedir alterações indesejadas aos dados (ex: modificação por alguém que não está autorizado a alterar a informação)

- Disponibilidade, medidas em vigor para prevenir ou pôr termo a incidentes de perda de acesso aos dados (ex: evitar as consequências de uma pessoa autorizada ou de um sistema interligado não poder utilizar o serviço, quando necessário, dentro do período de serviço estabelecido e anunciado pela organização)

- Rastreabilidade, medidas em vigor para poder verificar, a posteriori, quem acedeu ou alterou determinadas informações.

- Autenticidade, medidas em vigor para poder verificar a veracidade da informação.

e) Outros controlos:

- Monitorização, medidas em vigor para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança dos sistemas de informação

- Violação de dados, processos internos para detetar e/ou tratar de incidentes de segurança e de violação de dados pessoais

f) Regulamentação e outras obrigações legais:

- O ativo está sujeito aos requisitos previstos no RJSC (sim/não)

- O ativo está sujeito aos requisitos previstos no RGPD (sim/não)

- O ativo está sujeito a requisitos previstos noutros regulamentos e obrigações legais (PCI-DSS, HIPAA, COSO, SOC1, SOC2, NERC, etc..) (sim/não)

3.2 Proposta: Normalização na determinação da categoria de criticidade de determinado ativo.

a) Os níveis de categorização da criticidade dos ativos deverão ser definidos como: Baixa, Média ou Alta.

b) A determinação da categoria de um ativo deve basear-se na avaliação do impacto que teria para a organização caso ocorresse um incidente que afetasse a segurança da informação ou dos sistemas. Essa avaliação deve incidir sobre o impacto que o incidente provocaria na capacidade da organização para:

- Atingir os seus objetivos

- Proteger os ativos ao seu cuidado

- Cumprir as suas obrigações diárias de serviço

- Respeitar a lei em vigor

- Respeitar os direitos das pessoas

c) A fim de poder determinar o impacto que teria para a organização caso ocorresse um incidente que afetasse a segurança da informação ou dos sistemas e, assim, de poder estabelecer a categoria do ativo, devem ser tidas em conta as dimensões de segurança estabelecidas em 3.1.d):

- Confidencialidade (C)

- Integridade (I)

- Disponibilidade (D)

- Rastreabilidade (R)

- Autenticidade (A)

d) Um ativo pode ser afetado em uma ou mais das suas dimensões de segurança. Cada dimensão de segurança afetada deve ser atribuída a um dos seguintes níveis: Baixa, Média ou Alta. Se uma dimensão de segurança não for afetada, não deve ser atribuída a nenhum nível (N/A):

- Nível Baixo: a ser utilizado quando as consequências de um incidente de segurança que afete qualquer uma das dimensões de segurança são de prejuízo limitado para as funções da organização, para os seus ativos ou para as pessoas afetadas.

- Nível Médio: a ser utilizado quando as consequências de um incidente de segurança que afete qualquer uma das dimensões de segurança resultarem em danos graves para as funções da organização, para os seus ativos ou para as pessoas afetadas.

- Nível Alto: a ser utilizado quando as consequências de um incidente de segurança que afete qualquer uma das dimensões de segurança resultarem em danos muito graves para as funções da organização, para os seus ativos ou para as pessoas afetadas.

e) Para a determinação do nível de criticidade de um ativo:

- Um ativo deve ser classificado como Alto se alguma das suas dimensões de segurança atingir o nível Alto.

- Um ativo deve ser classificado como Médio se alguma das suas dimensões de segurança atingir o nível Médio, e nenhuma atingir um nível superior.

- Um ativo ser classificado como Baixo se alguma das suas dimensões de segurança atingir o nível Baixo, e nenhuma atingir um nível superior.

4. Normalização de tipologias e de métricas para melhoria da análise situacional integrada, no âmbito da gestão de ciberincidentes

A avaliação da implementação, eficácia e eficiência do processo de gestão de ciberincidentes necessita de ser alavancada em métricas e indicadores adequados, de forma ao que, quer da parte operacional quer da direção da organização, possam ser efetuados acompanhamentos corretos do processo de gestão bem como identificar tendências e variações não previstas. Ao nível da análise situacional nacional, também é importante uma normalização da taxonomia de incidentes.

Assim, e bem, na regulamentação do RJSC está previsto que "*as entidades devem elaborar um relatório anual que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:*

b) Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;"[8].

4.1 Proposta: Atualização da taxonomia de incidentes para melhor enquadramento do "*tipo dos incidentes*" a reportar, com introdução de novas tipologias de ameaças às previstas na alínea a), do n.º 3 do art.º 10.º do Decreto-Lei n.º 65/2021, de 30 de julho, com inclusão das seguintes tipologias de ameaças identificadas na ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management, no seu Anexo C (Examples of typical threats):

vi) Ações não autorizadas

vii) Falha técnica

viii) Perda de serviços essenciais

4.2 Proposta: Atualização da taxonomia de incidentes para melhor enquadramento do "*tipo dos incidentes*" a reportar, com a introdução da tipologia de "fontes de ameaça humana" alinhadas com a ISO/IEC 27005:2011 - Information technology -

[8] N.º 1 do art.º 8.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021

Security techniques - Information security risk management, no seu Anexo C (Origin of threats), e inclusão

i) Hacker

ii) Criminoso informático

iii) Terrorista

iv) Espionagem industrial

v) Ameaça interna (funcionários mal treinados, descontentes, maliciosos, negligentes, desonestos ou demitidos)

4.3 Proposta: Adoção de métricas relativas a ciberincidentes[9], para melhor enquadramento da "*Estatística trimestral de todos os incidentes*" a reportar.

a) Métrica **M1**

- Indicador: Âmbito do sistema de gestão de ciberincidentes

- Objetivo: Saber se todos os ativos estão abrangidos pelo serviço

- Método: Contabilizam-se quantos ativos estão sob gestão

Fórmula: # ativos sob gestão / # número total de ativos

- Objetivo = 100%

b) Métrica **M2**

- Indicador: Resolução de ciberincidentes que afetem ativos com nível de criticidade Alta

- Objetivo: Ser capaz de resolver rapidamente incidentes de alto impacto

- Método: Mede-se o tempo (T) necessário para resolver um incidente com impacto nos ativos de categoria Alta, ie, desde que se identifica até à sua resolução.

- Objetivo: T = 0.

c) Métrica **M3**

[9] As métricas propostas foram adaptadas do CCN-STIC 817 - Esquema Nacional de Seguridad - Gestión de ciberincidentes, Centro Criptológico Nacional, Espanha

- Indicador: Resolução de ciberincidentes que afetem ativos com nível de criticidade Médio

- Objetivo: Ser capaz de resolver rapidamente incidentes de impacto médio

- Método: Mede-se o tempo (T) necessário para resolver um incidente com impacto nos ativos de categoria Média, ie, desde que se identifica até à sua resolução.

- Objetivo: T = 0.

d) Métrica **M4**

- Indicador: Estado de encerramento dos incidentes

- Objetivo: Ser capazes de gerir ciberincidentes

- Método: Mede-se o número de incidentes que foram encerrados sem resposta.

Fórmula: # incidentes de segurança encerrados sem resposta / # número total de incidentes reportados

- Objetivo: <10%.