Encontro IPQ – RGPD Presente e Futuro

Mesa redonda: A Segurança do Tratamento e da Informação nas Organizações

VASCO SCHIAPPA, AUDITOR SISTEMAS DE INFORMAÇÃO, DIRETOR BDO PORTUGAL

Sobre o orador: Vasco Schiappa

- Diretor da BDO (5.ª maior firma/rede de auditoria e consultoria em Portugal e no mundo)
- Head do Departamento de Information Systems Audit da BDO
- 25 anos de experiência (sempre na BDO) em auditoria e consultoria de sistemas e segurança da informação e também em auditoria financeira
- Certified Information Systems Auditor (CISA), ISO 27001 Lead Auditor
- Cybersecurity Fundamentals, Rochester Institute of Technology certificate of achievement
- Revisor Oficial de Contas
- Conhecimentos e experiência em frameworks relevantes de IT: COBIT, ITIL, ISO 20000, ISO 27001/27002, ISO 22301, ISO 27005, ISO 29100, BS 10012, ISACA, IIA - GTAG - Global Technology Audit Guides, CMMI - Capability Maturity Model Integration, NIST - National Institute of Standards and Technology, ISF - Information Security Forum, PCI/DSS – Payment Card Industry / Data Security Standards, CIS – Center for Internet Security, ENISA, entre outros.
- RGPD: Larga experiência (mais de 40 projetos) em projetos de diagnóstico, Compliance e implementação do RGPD, na parte de segurança do tratamento e medidas técnicas e organizativas relacionadas com IT
- RGPD: Orador em diversas conferências e eventos promovidos pela BDO na divulgação do RGPD e Segurança do Tratamento

3 anos passados, na Área de Segurança da Informação

. O que fizeram o Estado e as organizações?

. Podem os titulares de dados estar confortados quanto à segurança dos seus dados pessoais?

. E agora, o que falta fazer?

CIBERSEGURANÇA É JÁ LEVADA A SÉRIO?

Segurança do tratamento e RGPD – Num relance

INTEGRIDADE E CONFIDENCIALIDADE
6º PRINCÍPIO (Artigo 5.º, n.º 1, alínea f)

"Tratados de uma forma que garanta a sua segurança, a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas"

EXATIDÃO
4.º PRINCÍPIO (Artigo 5.º, n.º 1, alínea d)

"Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora"

LIMITAÇÃO DA CONSERVAÇÃO
5.º PRINCÍPIO (Artigo 5.º, n.º 1, alínea e)

"Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados"

Segurança do tratamento e RGPD – Num relance

SEGURANÇA DO TRATAMENTO
(Artigo 32.º) - um artigo com 4 números, que pode implicar a implementação de dezenas senão centenas de controlos

1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

a) **Pseudonimização e a cifragem** dos dados pessoais;

b) **confidencialidade, integridade, disponibilidade e resiliência** dos sistemas e dos serviços de tratamento;

c) **restabelecer** a disponibilidade e o acesso no caso de um incidente físico ou técnico;

d) **testar, apreciar e avaliar** regularmente a eficácia das medidas técnicas e organizativas"

Segurança do tratamento e RGPD – Num relance

OUTROS ARTIGOS RELACIONADOS COM TI

- proteção de dados desde a conceção e por defeito (artigo 25.º)
- notificação violações de dados pessoais às autoridades de controlo (artigo 33.º)
- comunicação violação de dados pessoais aos titulares dos dados (artigo 34.º)
- avaliação de impacto sobre a proteção de dados (artigo 35.º)
- Direito à portabilidade (artigo 17.º)
- Direito ao apagamento (artigo 20.º)
- Consentimento (artigo 7.º)

O que foi feito? Portugal

• Estado: Lei de execução do RGPD (ainda por sair – junho 2019?) – na área da segurança da informação, o projeto de lei prevê: (i) Portaria (Saúde e Justiça) a aprovar medidas e requisitos técnicos mínimos de segurança inerentes ao tratamento de dados de saúde e genéticos; (ii) violação das regras de segurança do artigo 32.º como contraordenação grave; (iii) acesso indevido e desvio de dados punido com pena de prisão até um ano ou pena de multa até 120 dias (podendo ir ao dobro); (iv) viciação ou destruição de dados

• Estado: RCM 41/2018 - requisitos técnicos mínimos das redes e sistemas de informação (administração direta e indireta do Estado - a aplicar a partir de out2019)

• Estado: Lei 47/2018 - regime jurídico da segurança do ciberespaço, transpondo a NIS Directive (administração pública, operadores de infraestruturas críticas, operadores de serviços essenciais, prestadores de serviços digitais, outras entidades que utilizem redes e sistemas de informação (requisitos de segurança e de normalização ainda não foram definidos em legislação própria; valor máximo de contra-ordenação de 50k€)

O que foi feito? Portugal

• Estado/CNPD:

(i) Documento de 10 medidas (28jan17);

(ii) Regulamento n.º 1/2018 - lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD-DPIA) – 16out18;

(iii) Modelo de registo das atividades de tratamento (art. 30.º) – jan19;

(iv) Directrizes: n.º1/2018 Disponibilização de dados pessoais dos estudantes, dos docentes e demais trabalhadores no sítio da Internet das instituições de ensino superior (02out18); n.º 1/2019 Tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político (25mar19);

(v) a partir de 25mai18: 308 inspeções; 610 processos contraordenacionais; 22 coimas no valor total de 409k€ (maior parte reporta-se a factos antes do RGPD, pelo que se aplica o regime de coimas da LPDP)

A CNPD, ATUALMENTE CONTA COM UM QUADRO DE 22 PESSOAS

O que foi feito? Lá fora - exemplos a seguir?

- Espanha/AEPD:

(i) Guias práticos: GUIA PRÁCTICA DE Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD; Guía para la gestión y notificación de brechas de seguridad; Guía práctica para LAS Evaluaciones de Impacto en la Protección de LOS datos sujetas al RGPD

(ii) Ferramentas: “Facilita RGPD” (para PMEs); “Informa RGPD”

- Espanha/CCN (Centro Criptológico Nacional):

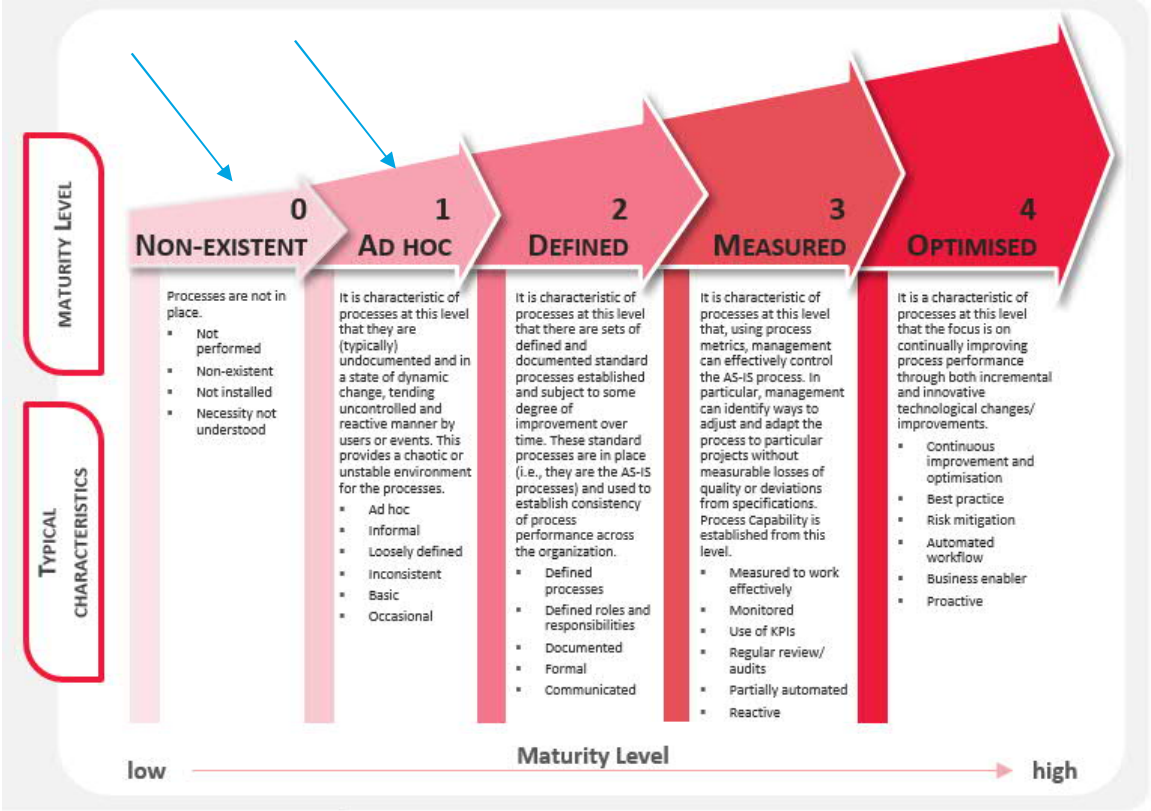
O que foi feito? Lá fora - exemplos a seguir?

- UK/ICO/NCSC:

(i) Guias: IT security top tips; IT asset disposal for organisations; A practical guide to IT security; Protecting personal data in online services – learning from the mistakes of others; Bring your own device (BYOD); Cloud computing; Encryption; 10 Steps to Cyber Security; The Cyber Essentials scheme; Risk Management Collection; CyberAware; 'Cybersecurity – what small businesses need to know'

(ii) Certificações NCSC: "Cyber Essentials Scheme"

O que foi feito? As organizações – estágio maturidade



Note: This maturity model is based on the Capability Maturity Model (CMM) Standard

Podem os titulares de dados estar confortados quanto à segurança dos seus dados pessoais?

Portugal é o segundo país do mundo com mais utilizadores atacados com spam e phishing

A fatia de utilizadores atacados com spam e phishing cresceu em Portugal, colocando o país em segundo lugar a nível mundial. À frente dos portugueses mantêm-se apenas os utilizadores brasileiros.

Podem os titulares de dados estar confortados quanto à segurança dos seus dados pessoais?

- O Ransomware continua a impactar fortemente as Organizações
- A Engenharia Social continua a ser o motor de muitos ataques
- O DDoS continua a ser uma ferramenta de ataque contra organizações públicas e privadas
- A nova legislação (RGPD e NIS Directive) poderá levar a um aumento na ciber-extorsão

Ransomware retains its dominance

Even though the growth of ransomware is beginning to slow, ransomware is still overtaking banking Trojans in financially-motivated malware attacks, a trend anticipated to continue over the following years. In addition to attacks by financially motivated criminals, a significant volume of public reporting increasingly attributes global cyber-attacks to the actions of nation states. Mobile malware has not been extensively reported in 2017, but this has been identified as an anticipated future threat for private and public entities alike.

Illegal acquisition of data following data breaches is a prominent threat. Criminals often use the obtained data to facilitate further criminal activity. In 2017, the biggest data breach concerned Equifax, affecting more than 100 million credit users worldwide. With the EU GDPR coming into effect in May 2018, the reporting of data breaches is now a legal requirement across the EU, bringing with it hefty fines and new threats and challenges.

Social engineering still the engine of many cybercrimes

The significance of social engineering for cyber-dependent and cyber-enabled crime continues to grow. Phishing via email remains the most frequent form of social engineering, with vishing (via telephone) and smishing (via SMS) less common. Criminals use social engineering to achieve a range of goals: to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments, or convince the victim to proceed with any other activity against their self-interest, such as transferring money or sharing personal data.

DDoS continues to plague public and private organisations

Criminals continue to use Distributed-Denial-of-Service (DDoS) attacks as a tool against private business and the public sector. Such attacks are used not only for financial gains but for ideological, political or purely malicious reason. This type of attack is not only one of the most frequent (second only to malware in 2017), it is also becoming more accessible, low-cost and low-risk.

New legislation may lead to an increase in cyber-extortion

It is not only the NIS Directive that will lead to an increase in reporting of data breaches. The General Data Protection Regulation which came into effect in May 2018 requires the reporting of breaches of personal data within 72 hours. Moreover, such breaches can result in substantial fines; potentially EUR 20 million or 4% of the company's global annual turnover, whichever is higher[50]. This may give rise to scenarios where hackers may try to extort companies over their data loss. While this is not new, it may be that the hacked companies would rather pay a smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by their competent authority. Such payments however, will only fund further attacks and other criminal activity, and are no guaranteed that the attacker will not disclose or otherwise exploit the information.

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018

Podem os titulares de dados estar confortados quanto à segurança dos seus dados pessoais?

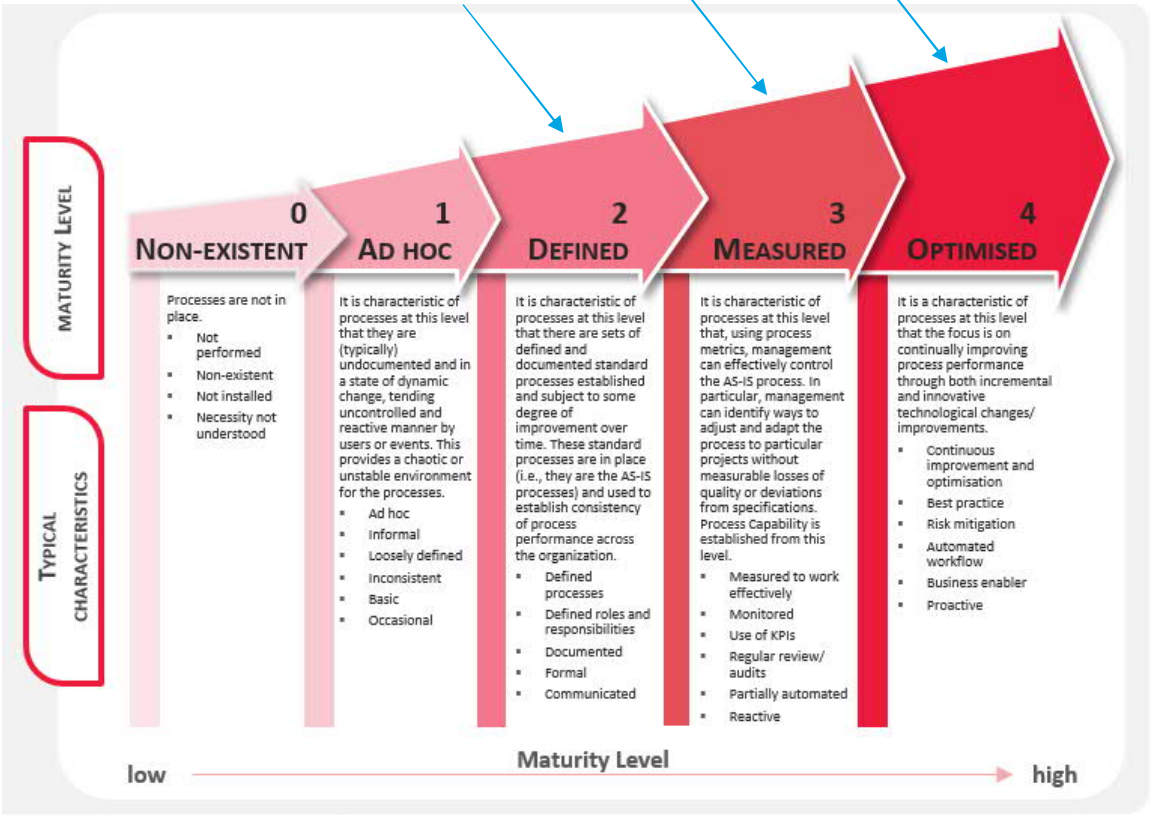
"There are only two types of organizations: those that know that they've been hacked and those that don't yet know"

Crowdstrike's Dmitri Alperovitch

O que falta agora fazer?

LONGO CAMINHO

O que falta agora fazer?



Note: This maturity model is based on the Capability Maturity Model (CMM) Standard

Encontro IPQ – RGPD Presente e Futuro

Mesa redonda: A Segurança do Tratamento e da Informação nas Organizações

VASCO SCHIAPPA, AUDITOR SISTEMAS DE INFORMAÇÃO, DIRETOR BDO PORTUGAL
vasco.schiappa@bdo.pt