Microsoft

Estudo

Estado da Cibersegurança em Portugal

2023-2024

Enquadramento

Num mundo cada vez mais digital e em profunda transformação, a segurança cibernética desempenha, mais do que nunca, um papel crucial na proteção de dados, pessoas, organizações e governos.

Para compreender o Estado da Cibersegurança em Portugal e estando agendada para outubro de 2024 a entrada em vigor da nova diretiva NIS2 (*Network and Information Security Directive*), a Microsoft promoveu a condução de um estudo junto de decisores de 184 organizações a operar a nível nacional, com o objetivo de apurar:

1. Grau de maturidade e práticas de cibersegurança implementadas nas organizações;
2. Como pode a IA ajudar as organizações nacionais a serem ciberneticamente mais eficientes;
3. Níveis de conformidade das organizações com a NIS2.

Os dados foram recolhidos entre 22 e 29 de setembro de 2023, via painel Netsonda, através de um questionário aplicado a vários quadros diretivos e intermédios (N=184), com poder de decisão na organização, contemplando um total de 17 questões de resposta simples e múltipla e ainda um conjunto de questões sociodemográficas e organizacionais, com vista à filtragem e caracterização da amostra.

Construir um futuro seguro e próspero

O mundo enfrenta crescentes ameaças à segurança, no mundo físico, e também no digital. O crescimento exponencial do número de ciberataques, que tem sido acompanhado por um grau de complexidade e sofisticação progressivos, colocam sérias ameaças a infra-estruturas críticas e serviços na nuvem.

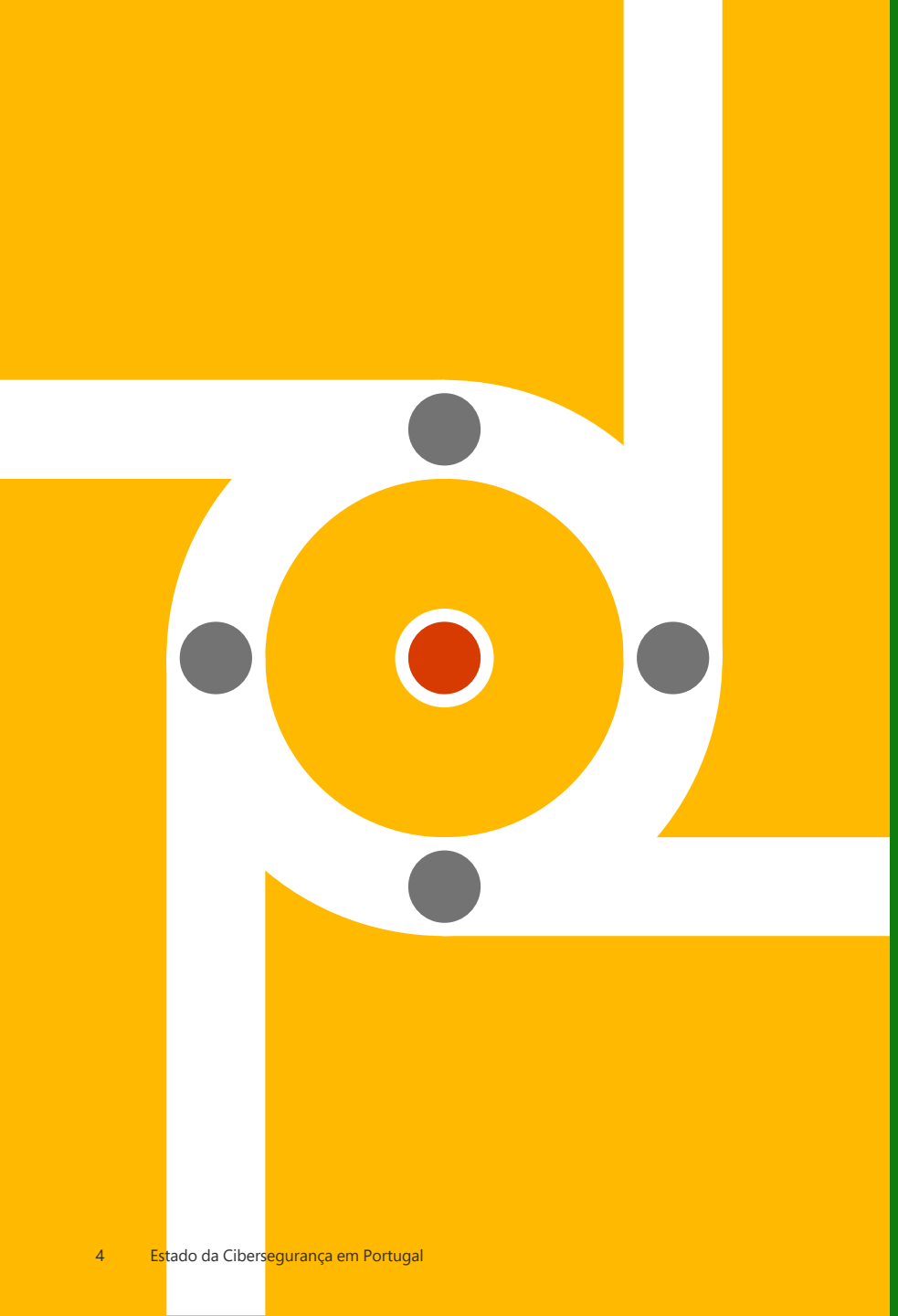
Perante a urgência de uma nação coordenada, as equipas de defesa estão a responder à necessidade de melhoria da segurança, com as organizações a investir e a trabalhar para criar resiliência a longo prazo. Muitos fornecedores de *software* estão a tomar medidas para melhorar a cibersegurança dos seus produtos e serviços, criando novas ferramentas para ajudar os clientes a defenderem-se dos atacantes, e Governos de todo o mundo estão a educar os seus cidadãos para compreender os riscos das ciberameaças e como os combater.

O ano de 2023 ficou marcado, não só por este alarme, mas também pelo crescimento exponencial da Inteligência Artificial. E com este progresso, esta tornou-se uma poderosa ferramenta de duas faces: de ataque e de defesa.

Vemos os atacantes a usar a IA como arma para melhorar as mensagens de *phishing*, desenvolver código malicioso e permitir outros abusos da tecnologia, como a criação de *deep fakes*. Mas a IA é, também, e essencialmente, uma componente fundamental numa defesa bem-sucedida, sendo capaz de gerar recomendações em linguagem natural a partir de dados complexos, que resultam numa maior eficácia e capacidade de resposta no controlo de ameaças, ajudando as organizações a prevenirem e a parar os ataques à velocidade de uma máquina.

Compreendendo que a velocidade, a escala e a sofisticação crescente dos ciberataques exigem uma compreensão e resposta global, é importante conhecer os desafios nacionais, oferecendo uma análise, possíveis diagnósticos e recursos para que possamos tomar, em conjunto, os passos necessários para construir para nós, e para as nossas organizações, um futuro mais seguro, resiliente e próspero.

Luís Rato
Diretor Nacional de Tecnologia da Microsoft Portugal



Sumário Executivo

Investir em segurança cibernética tem sido uma prioridade efetiva para a maioria das organizações a operar em Portugal. E ainda que os valores de investimento possam diferir de organização para organização, há uma certeza comum: **o investimento deve começar na formação e consciencialização dos colaboradores.**

Para as organizações que já investiram na implementação de medidas de segurança cibernética, o esforço sai compensado e tem um impacto mensurável: **menor exposição a incidentes e menores casos associados a perda de dados e a danos financeiros.**

Mas há ainda um longo caminho a percorrer por grande parte das organizações, nomeadamente, em matéria de conformidade com a nova diretiva NIS2. Um cenário que antecipa indefinições estratégicas, possíveis lacunas do ponto de vista de comunicação, que urge ser colmatado e que sai reforçado com o recurso a consultoria externa, por uma fatia considerável das organizações a nível nacional.

Grau de maturidade e práticas de cibersegurança nas organizações

Olhando em profundidade para o tecido empresarial português, é notório o reconhecimento que a segurança cibernética tem na proteção global da organização e da sua atividade, seja qual for a sua dimensão e setor de atividade. Não será, por isso, de estranhar que **45%** das organizações tenha um investimento projetado em cibersegurança, no futuro, começando desde logo pelo reforço da consciencialização e formação dos Colaboradores, segundo **84%** dos inquiridos.

Igualmente importante será o investimento em:

Avaliações regulares de risco cibernético	**69%**
Auditorias de segurança	**66%**
Monitorização de ameaças em tempo real	**66%**

45%

das organizações
terá um investimento projetado
em cibersegurança no futuro

A existência de uma equipa de:

Security Operations (SecOpps) interna	**53%**
Equipa de práticas de *IT Business Continuity*, de planos de resposta e mitigação, de uma estrutura de governança	**50%**
Parceiros especializados (*SOCasaService*) para conduzir as operações de segurança	**45%**

serão igualmente áreas a considerar, de acordo com as organizações auscultadas.

Grau de maturidade e práticas de cibersegurança nas organizações

Já no que toca às principais ameaças cibernéticas que se impõem às organizações:

70%

dos inquiridos destaca o *Phishing*

63%

dos inquiridos destaca os *softwares* maliciosos

com encriptação de dados e pedido de resgate.

29%

dos inquiridos destaca os ataques de negação de serviço DDoS

pela sua capacidade de explorar vulnerabilidades nas redes e dispositivos programáveis da organização e, desta forma, perturbar os serviços e recursos das aplicações.

Chegada a hora de investir, a grande maioria dos inquiridos **(41%) assume que o investimento ficará abaixo dos 10.000€**, **20% baliza o investimento entre 10.000€ e 50.000€**, **enquanto uma percentagem considerável (35%) desconhece por completo os investimentos previstos**.
Um cenário que reforça alguma indefinição estratégica do lado das organizações.

Grau de maturidade e práticas de cibersegurança nas organizações

Para lá das previsões, há um esforço já concretizado pelas organizações a nível nacional que importa destacar: **50%** investiu mais em cibersegurança nos últimos anos, nomeadamente com a implementação de:

Antivírus e *malware*	**81%**
Medidas de autenticação fortes para o acesso a sistemas críticos	**71%**
Firewalls	**61%**
Autenticação *multi-factor*	**37%**
Criptografia de dados, para proteger os ativos da empresa	**36%**

Mas mesmo para as organizações que estiveram expostas a incidentes cibernéticos, a grande maioria **(68%)** afirma nunca ter havido perda financeira associada e **17%** assume mesmo desconhecer e existência de impacto financeiro. **62%** dos inquiridos refere ainda nunca ter havido perda de dados resultantes de incidentes cibernéticos, contrariamente a apenas **24%** que assume já ter acontecido. A comunicação às autoridades competentes é também um procedimento apontado pela maioria **(65%)**, contrariamente a apenas **16%** que não privilegiou esta conduta.

O papel da IA na segurança cibernética

Assim como os ataques cibernéticos evoluem e se tornam cada vez mais sofisticados de dia para dia, também as novas tecnologias têm procurado evoluir para estar um passo à frente das ameaças. A Inteligência Artificial (IA) materializa esta premissa, sendo atualmente capaz de recolher e analisar uma quantidade de dados cada vez maior e de os correlacionar para, assim, conseguir apoiar as organizações na identificação de vulnerabilidades, na gestão de incidentes de segurança cibernética e na criação de um ecossistema mais seguro e resiliente.

Saiba mais sobre as vantagens das ferramentas de segurança alimentadas por IA generativa **aqui.**

65 triliões
de sinais de alerta sintetizados diariamente

São mais de 75O mil milhões de sinais de alerta por segundo, sintetizados utilizando análises de dados sofisticados e algoritmos de IA para compreender e proteger contra ameaças digitais e ciberatividade criminosa.

+10.000
especialistas em segurança e inteligência

Mais de 1O.OOO engenheiros, analistas, cientistas de dados, peritos em cibersegurança, investigadores, analistas geopolíticos e *frontline responders* em todo o mundo.

4.000
ataques de identidade bloqueados por segundo

4.OOO ameaças de autenticação bloqueadas por segundo.

+15.000
parceiros no ecossistema de segurança da Microsoft

Mais de 15.OOO parceiros com soluções especializadas que aumentam a ciber-resiliência dos clientes Microsoft.

300+
agentes de ameaça cibernética rastreados

A plataforma Microsoft *Threat Intelligence* evoluiu para detetar mais de 3OO agentes únicos, incluindo de 16O estados-nação, 5O grupos de *ransomware* e centenas de outras tipologias.

+100.000
domínios removidos

Mais de 1OO.OOO domínios utilizados por informações sobre segurança e ameaças cibernéticas. cibercriminosos foram removidos, incluindo mais de 6OO por agentes de estados-nação.

135 milhões
de dispositivos geridos

135 milhões de dispositivos geridos que fornecem mais de 1OO.OOO domínios utilizados por informações sobre segurança e ameaças cibernéticas.

*Dados constantes do Microsoft *Digital Defense Report* e referentes ao ano fiscal de 2023 da Microsoft, salvo indicação em contrário.

O papel da IA na segurança cibernética

Mas muito embora a IA possa desempenhar um papel absolutamente estratégico na evolução da segurança cibernética, a sua integração nos processos de segurança é ainda uma realidade longínqua para a maioria das organizações.

54% dos inquiridos auscultados afirma não utilizar soluções de segurança com recurso a IA.

As organizações que já o fazem – **21%** – recorrem a competencias de:

Reporte de incidentes de segurança	**66%**
Cyber intelligence e a exposição a ameaças	**61%**
Sistemas preditivos de ataque	**49%**
Resposta a incidentes	**46%**

Uma decisão que caberá, seguramente, ao Diretor(a) de Segurança de Informação/ CISO, função que **45%** dos inquiridos afirma integrar já a estrutura corporativa, mas que em percentagem pouca distancia da realidade de **43%** das organizações que referem não ter ainda esta função.

Níveis de conformidade das organizações com a NIS2

18 Setores

18.000 Empresas

A nova NIS2 é a legislação mais abrangente da União Europeia em matéria de cibersegurança e constitui um importante passo em frente no estabelecimento de um conjunto de requisitos, obrigações específicas e de medidas mais harmonizadas entre Estados-membros. Compreender a sua aplicação e o seu impacto constitui igualmente uma oportunidade para que as organizações possam acelerar a sua jornada de transformação digital, com eficiência do ponto de vista da sua segurança cibernética.

Alcançar a conformidade com a NIS2 é, por isso, um processo que deve fluir de forma alinhada e compreendendo três pilares fundamentais: Pessoas, Planeamento e Parceiros, de acordo com o **Guia NIS2** para Líderes, da Microsoft.

Setores altamente críticos

- Energia
- Transportes
- Banca
- Infraestruturas do Mercado Financeiro
- Setor da Saúde
- Água Potável
- Águas Residuais
- Infraestruturas Digitais
- Gestão de Serviços IT
- Administração Pública
- Setor Espacial

Setores críticos

- Alimentar
- Gestão de Resíduos
- Químicos
- Serviços Postais e Correio Rápido
- Fabrico de Dispositivos Médicos
- Fornecedores Digitais
- Organismos de Investigação

Níveis de conformidade das organizações com a NIS2

Pessoas

Investir ativamente na capacitação dos colaboradores, envolvendo de forma estruturada e alinhada todos os níveis hierárquicos da organização. Tal implica garantir o acesso às ferramentas certas, independentemente da função e modelo de trabalho – presencial, remoto ou em trânsito. Fazê-lo, integrando IA, assegurará avanços mais rápidos e uma estrutura robustamente mais capaz de mitigar as ameaças cibernéticas.

Planeamento

A diretiva NIS2 exigirá às organizações a existência de planos preventivos e reativos para incidentes cibernéticos e que envolve, forçosamente, a identificação cirúrgica das vulnerabilidades e a implementação de medidas de proteção em conformidade. Definir e implementar estes planos implicará avaliações de risco, envolvendo a segurança de toda a cadeia de fornecimento, bem como a definição e implementação de planos de contingência, através da integração de ferramentas e processos.

Parceiros

À medida que o cenário de ameaças evolui, nenhuma organização pode mitigar eficazmente a ameaça e garantir a comunicação exata e atempada de incidentes se trabalhar num silo. Trabalhar com parceiros certificados representa, por isso, um passo essencial para maximizar os controlos de segurança e para que as organizações possam modernizar a sua abordagem à cibersegurança.
Ao preparar-se para a conformidade com a NIS2, as organizações estão também a reforçar a sua credibilidade e confiança junto de clientes, parceiros, fornecedores e demais *stakeholders* estratégicos à sua atividade.

Níveis de conformidade das organizações com a NIS2

Mas estarão as organizações nacionais cientes e preparadas para o impacto da NIS2?

53% dos inquiridos acredita que sim e **70%** vai mais longe, defendendo que a organização já se encontra em conformidade com a nova diretiva. Há ainda as organizações que assumem já ter definido planos de ação nesse sentido **(73%)** e as que já concretizaram efetivamente ações em prol da conformidade **(62%)**. Porém, há ainda uma fatia significativa **(62%)**, que afirma ter recorrido a consultoria externa para traçar a sua estratégia e para robustecer a organização de maiores níveis de conhecimento, tal é o desconhecimento sobre as implicações da nova diretiva na atividade global da organização **(40%)**.

Medidas de Gestão de Riscos da NIS2

1. Políticas de análise de risco e de segurança dos sistemas de informação;
2. Tratamento de incidentes cibernéticos;
3. Continuidade da atividade, através da gestão de cópias de segurança, recuperação de desastres e gestão de crises;
4. Segurança da cadeia de abastecimento, incluindo aspetos relacionados com a segurança das relações entre cada entidade e os seus fornecedores diretos ou prestadores de serviços;
5. Segurança em rede, nomeadamente na aquisição, desenvolvimento e manutenção de redes e sistemas de informação, incluindo o tratamento e a divulgação de vulnerabilidades;
6. Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;
7. Práticas básicas de higiene cibernética e formação em cibersegurança;
8. Políticas e procedimentos relativos à utilização da criptografia e, se for caso disso, de encriptação;
9. Segurança dos recursos humanos, políticas de controlo do acesso e gestão de ativos;
10. A utilização de soluções de autenticação *multi-factor* ou de autenticação contínua, de comunicações seguras de voz, vídeo e texto e de sistemas seguros de comunicações de emergência, quando apropriado.

Níveis de conformidade das organizações com a NIS2

Se olharmos agora para os sistemas de gestão de informação e risco cibernético exigidos pela NIS2 e que se encontram presentemente ativos nas organizações:

51%
assume que a gestão de risco e informação é o principal ativo.

49%
dos inquiridos refere ainda a comunicação e gestão de incidentes.

48%
dos inquiridos a contratação de formação em cibersegurança a entidades externas.

41%
dos inquiridos aponta a encriptação e autenticação *multi-factor*.

16%
dos inquiridos destaca a dimensão de *Business Continuity*.

23%
Do total de inquiridos, desconhece por completo o esforço feito pela sua organização.

Recomendações

O **desconhecimento apontado por alguns inquiridos** relativamente à estratégia de investimento da sua organização e às medidas implementadas para tornar a segurança cibernética efetiva conduz a empresa a uma **maior exposição ao risco**, impactando simultaneamente o envolvimento dos seus colaboradores na proteção global da organização e dos seus dados.

Torna-se, por isso, **imperativo investir ativamente na comunicação, trabalhando os seus fluxos de forma alinhada e com um propósito claro:** maior alinhamento na partilha de informação; maior mobilização e envolvimento na execução da estratégia; maior compromisso para alcançar as metas estabelecidas.

As Pessoas são "a primeira e última linha de defesa de uma organização".

- Criação de uma cultura de cibersegurança;
- Abordagem colaborativa e positiva, com modelos formativos envolventes e conteúdos compreensíveis para todos os níveis hierárquicos e funcionais;
- Conhecimento real e partilhado sobre o impacto resultante de incidentes cibernéticos e orientações estratégicas sobre como detetar, agir, corrigir e mitigar os incidentes.

Uma boa formação pode reduzir em **40%** **a vulnerabilidade de uma empresa ao *phishing*!**

Recomendações

Compreender quais as melhores práticas para um comportamento seguro será um passo fundamental para que cada colaborador possa fazer melhor a sua parte e, conjuntamente, tornar a organização mais ciberinteligente. **Assim, há cinco dimensões básicas da cibersegurança que qualquer organização, independentemente da sua dimensão, deve ter asseguradas:**

1

Ativar a autenticação *multi-factor*

Escolha uma opção MFA com menos atrito e ative-a para ajudar a proteger dados sensíveis e sistemas críticos, em vez de a aplicar a cada interação. Utilize políticas de acesso condicional, autenticação de passagem e início de sessão única (SSO) no acesso e partilha de ficheiros não críticos ou calendários na rede empresarial.
Com **a MFA ativada pode evitar 99,9% dos ataques às suas contas.**

2

Aplicar os princípios de confiança zero

A confiança zero é a pedra angular de qualquer plano de resiliência que limite o impacto numa organização. Assegure a monitorização constante, assumindo que o atacante pode e vai agir a qualquer momento, podendo ser bem sucedido. Limite ainda o acesso de um ativo potencialmente comprometido com *just-in-time* e *just-enoughaccess* (JIT/JEA) e políticas baseadas em *isk*. Só deve permitir o privilégio necessário para aceder a um recurso a nada mais.

3

Utilizar um *anti-malware* moderno

Utilize um *anti-malware* de deteção e resposta alargadas e implemente *software* para detetar e bloquear automaticamente os ataques e fornecer informações sobre as operações de segurança.

Recomendações

4

Manter os sistemas atualizados

Os sistemas não corrigidos e desatualizados são uma das principais razões pelas quais muitas organizações são vítimas de um ataque. Certifique-se de que todos os sistemas são mantidos atualizados, incluindo o *firmware*, o sistema operativo e as aplicações. Aplique *patches* e altere as palavras-passe e portas SSH predefinidas. Elimine ligações desnecessárias à Internet e restrinja o acesso remoto, negando a utilização de serviços VPN. Dispositivos IoTe as redes OT devem ainda ser isolados das redes informáticas corporativas através de *firewalls*.

5

Proteger os dados

Saiba quais são os dados importantes, onde estão localizados e confirme se os sistemas corretos são implementados. Só assim conseguirá implementar a proteção adequada.

Microsoft

Estudo

Estado da Cibersegurança em Portugal

2023-2024