newsletter

cyber&data protection IP

Politécnico de Viseu · Politécnico da Guarda · ipvc Instituto Politécnico de Viana do Castelo

CIBERSEGURANÇA

IPG ALERTA PARA IMPORTÂNCIA DA COOPERAÇÃO ENTRE PAÍSES NO COMBATE AO CIBERCRIME

O Instituto Politécnico da Guarda – IPG realizou, no dia 2 de junho, a terceira edição da Conferência Internacional de Cibersegurança, a qual reuniu especialistas da área de Informática e da Cibersegurança, para discutir as estratégias de prevenção e a importância da coordenação internacional no combate ao crime informático. "A cooperação entre países e o trabalho em rede entre os gabinetes de segurança informática das empresas e organizações é fundamental para antecipar e evitar o cibercrime", afirmou Pedro Pinto, responsável pela cibersegurança do IPG.

"A garantia de redes seguras e sistemas mais resilientes passa pela partilha de conhecimento entre as organizações, mas sobretudo pela capacitação de quadros especializados e atualizados", afirmou Joaquim Brigas, presidente do IPG. "A área da cibersegurança é uma prioridade para o IPG. Recentemente estabelecemos uma parceria com a multinacional americana Fortinet, que prevê a instalação da sua academia no IPG e a formação de especialistas em cibersegurança."

O Politécnico da Guarda tem apostado na área da segurança informática, nomeadamente através de congressos, workshops e formações especializadas, tendo sido a primeira instituição de ensino superior do país a lançar um curso em Cibersegurança.

A importância da cooperação internacional no combate ao cibercrime, os quatro anos da aplicação do Regulamento Geral sobre a Proteção de Dados, a evolução da tecnologia quântica na cibersegurança e a importância da cibergurança nas cadeias

de distribuição, foram alguns dos temas em debate na conferência.

"A cibersegurança é extremamente importante devido à nossa dependência dos sistemas informáticos. A pandemia e a guerra na Ucrânia exacerbaram o número os ataques informáticos, obrigando a um maior investimento na área", afirmou Noel Lopes, coordenador da UTC de Informática do IPG. "Esta conferência veio trazer perspetivas de diferentes especialistas e métodos de atuação perante as vulnerabilidades dos sistemas de informação que serão, certamente, enriquecedoras para estudantes, docentes e técnicos."

A conferência teve inicio às 09h no Auditório dos Serviços Centrais do Politécnico da Guarda e contou com a participação do contra-almirante António Gameiro Marques, do Gabinete Nacional de Segurança, Jesús Martínez Martínez, da Universidade de Múrcia (Espanha), João Ferreira Pinto, encarregado da Proteção de Dados no Supremo Tribunal de Justiça, António Rio Costa, do Centro Nacional de Cibersegurança, e Victor Lobo, da Escola Universitária Militar da Universidade Nova de Lisboa, entre outros.

Fonte **POLITÉCNICO GUARDA**
Fotos **POLITÉCNICO GUARDA**

SECURNET ASSINA PROTOCOLO COM O POLITÉCNICO DA GUARDA

A tecnológica portuguesa Securnet irá instalar no Politécnico da Guarda um Centro de Competências. "A aposta nas tecnologias de informação já é uma vantagem competitiva desta Instituição de Ensino Superior do Interior!", afirmou o seu presidente, Joaquim Brigas.

A Securnet é uma empresa especializada em serviços avançados de consultoria, integração e manutenção. O IPG, garantiu Joaquim Brigas, irá continuar a sua grande aposta na área das Tecnologias de Informação: "Essa aposta já é, e será mais ainda no futuro, uma vantagem competitiva desta Instituição de Ensino Superior sediada no Interior!"

Embora o anúncio foi feito na abertura das Jornadas de Engenharia Informática de 2022, que decorreram no dia 4 de maio, o protocolo de cooperação foi assinado no dia 2 de junho, cerimónia integrada na terceira edição da Conferência Internacional de Cibersegurança.

PROTEÇÃO DE DADOS

METADADOS: O QUE SÃO, PARA QUE SERVEM E QUAIS OS PERIGOS

António Guimarães
(Jornalista da equipa de digital da CNN Portugal)

Quem pode consultar os nossos metadados? E quem está responsável por os armazenar? Sabia que desde 2017 ninguém fiscaliza esta questão? Um explicador sobre os metadados.

O Tribunal Constitucional (TC) veio declarar uma lei de 2008 inconstitucional, abrindo uma polémica relacionada com os metadados. Mas afinal, o que são os metadados, cujo chumbo do TC pode ditar uma revolução na Justiça portuguesa? A CNN Portugal elaborou um conjunto de perguntas e respostas para, com ajuda de especialistas, responder a todas as questões.

O que são metadados?

Os metadados são um conjunto de dados alargados que nos permitem obter determinadas informações. A advogada Elsa Veloso, especialista em Proteção de Dados, refere que estes dados dizem respeito a dados de tráfego, de localização e de dados conexos para identificar um determinado assinante ou utilizador. No fundo, são "todos os dados", sendo que meta significa além de, portanto, metadados são dados além dos dados, "informações que acrescem aos dados".

Dizem respeito a diferentes formas de comunicação: correio eletrónico, mensagens de texto, chamadas telefónicas. "Metadados é um conjunto alargado de dados que nos permite chegar a uma pessoa identificada ou identificável", explica Elsa Veloso. É possível saber com quem, durante quanto tempo e a partir de onde falou determinada pessoa.

No fundo, servem para tornar mais fácil a organização dos dados. É aquilo a que José Tribolet compara com uma espécie de catalogação. O professor jubilado de Sistemas de Informação do Instituto Superior Técnico faz uma analogia com um jornal: "Os metadados vão ser a informação sobre o objeto, não têm que ver com os conteúdos em si, mas com as datas, origem da coisa."

Para que servem os metadados?

Os metadados permitem uma espécie de catalogação de determinadas informações, podendo ser úteis na prevenção, investigação ou repressão de crimes graves, como vinha previsto na lei agora tornada inconstitucional.

"Num mar de informações conseguimos encontrar uma coisa com determinados atributos de forma rápida, porque existe um conjunto de indicadores, os metadados", explica José Tribolet.

Na sua conservação está prevista a investigação de crimes como terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

Quem faz a conservação e gestão dos metadados?

A conservação dos metadados é feita por um período de um ano, lembra Elsa Veloso, sublinhando que a conservação e gestão destes dados é feita pelas diferentes operadoras. Se as suas comunicações são feitas através da Vodafone, por exemplo, será essa operadora a conservar os seus dados.

"A Vodafone, a MEO ou a NOS dão-lhe oportunidade de fazer o envio de mensagens, de vídeos, de fotografias. Cada vez mais

usamos dados e menos telefone", indica a advogada, apontando que "todas as operadoras têm uma oferta integrada", sendo que "têm de guardar os dados todos dos seus clientes durante o período referido".

No entanto, é à Comissão Nacional de Proteção de Dados (CNPD) que compete a fiscalização do armazenamento destes dados, que atualmente está em suspenso. Aquele organismo disse, em 2017, que a lei viola o princípio da proporcionalidade e da necessidade, apontando ainda uma ingerência nos direitos fundamentais.

"A CNPD decidiu desaplicar a lei", refere Elsa Veloso, explicando que, assim, "deixou de fiscalizar". "Desde 2017, até hoje, não há fiscalização sobre a forma como estes dados são conservados ou a forma como é feito o acesso aos dados", sublinha.

Quem pode aceder aos metadados?

De forma legal, apenas os órgãos de polícia criminal, devidamente autorizados por um tribunal, podem aceder aos metadados dos utilizadores, explica Elsa Veloso. No entanto, a especialista fala em violações de dados cada vez mais frequentes, mediante acessos ilegais.

O que é e não é considerado metadados (Internet e comunicações móveis)?

Voltando à analogia do jornal, José Tribolet refere que todo o conteúdo inscrito numa notícia não é considerado metadados. O mesmo é dizer que o conteúdo das nossas conversas não será conhecido através dos metadados, que dizem apenas respeito a quem está a participar na chamada, bem como a duração e o local em que a mesma foi efetuada.

O mesmo se aplica às comunicações que utilizam texto. Por exemplo, o WhatsApp ou e-mail têm metadados associados, mas isso não quer dizer que sirvam para saber o que está a ser escrito. Como nas chamadas, os metadados dizem respeito apenas ao tempo em que a informação foi trocada, bem como quais os interlocutores da mesma, além da localização.

Quais os perigos dos metadados?

Elsa Veloso remete novamente para a CNPD, que deixou de fiscalizar, pelo que, atualmente, "não sabemos" o que está a acontecer a milhões de metadados.

"Os perigos são todos: se alguém souber para quem um jornalista liga a uma hora, podem saber as fontes desse jornalista. O mesmo na vida privada, e privacidade é igual a liberdade", afirma.

Este problema ganha ainda maior relevância, lembra a advogada, numa altura em que têm sido realizados vários ataques informáticos a empresas de telecomunicações, como foi o caso da Vodafone. "Há milhões e milhões de metadados que não sabemos como estão a ser armazenados."

"Todo este tipo de utilizações podem ser para coisas bondosas, mas também, de uma forma não controlada, para efeitos maliciosos", acrescenta José Tribolet.

O que é a Lei dos Metadados?

A Lei dos Metadados (Lei 32/2008) entrou em vigor em Portugal em 2008, na sequência de uma diretiva europeia de 2006, que visava a "conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações". A ideia partiu da necessidade de implementar medidas para combater o terrorismo em solo europeu.

O objetivo era monitorizar vários dados, como os descritos acima, para intercetar eventuais comunicações que pudessem constituir uma ameaça aos Estados-membros da União Europeia.

O presidente do Sindicato dos Magistrados do Ministério Público (SMMP) explica que esta lei "impunha às operadoras e aos fornecedores de serviços que conservassem os metadados durante o período de um ano", recorda Adão Carvalho.

Porque declarou o TC esta lei inconstitucional? E porque levou tanto tempo?

O TC declarou o artigo 4.° inconstitucional por entender que o mesmo viola o direito de privacidade dos cidadãos, uma vez que não visa apenas os suspeitos de crime, mas todos os cidadãos.

O presidente do SMMP lembra que a lei em causa tinha como "objeto da conservação [de dados] todos os cidadãos". "Ficavam todos com os dados conservados, e não só um grupo determinado."

Mas o problema vem de antes, mais concretamente de 2014. Nesse ano o Tribunal de Justiça da União Europeia (TJUE) recebeu uma queixa relativamente à diretiva, acabando por declará-la inválida, alegando que "infringia o direito fundamental ao respeito pela vida privada e à proteção de dados pessoais".

Adão Carvalho refere que em causa estavam direitos inscritos na Carta Fundamental, como o direito à autodeterminação informativa e o direito de privacidade dos dados.

"Também não estava prevista a notificação do fornecimento dos dados ao titular dos mesmos, e o TJUE entendia que isso tinha de ser feito", acrescenta.

De 2014 para 2022 foram oito anos. Porquê tanto tempo? É que, tal como o TJUE, também o TC funciona por pedidos de fiscalização. Adão Carvalho lembra que o podem fazer o Presidente da República, um determinado grupo de deputados ou a provedora de Justiça. Foi este último cenário que ocorreu em 2019, com aquela figura a pedir a fiscalização da Lei dos Metadados. Daí decorreu o tempo até à decisão do TC, agora conhecida.

"O TC teve de aceitar a interpretação do TJUE, designadamente a interpretação de que esta norma violava princípios constitucionais", afirma Adão Carvalho, apontando que esta é uma decisão complicada, porque "não conseguimos definir quem é criminoso a priori".

Na Alemanha, por exemplo, a alteração à lei foi realizada logo em 2015.

Quais as consequências? Podemos ter processos judiciais arquivados ou revertidos?

Adão Carvalho lembra que a decisão do TC não se refere a um possível efeito retroativo. De resto, o presidente do SMMP diz que, no seu entender, esta alteração nunca poderá vir a ser aplicada nos processos já transitados em julgado.

Situação diferente poderá ser a dos processos que ainda decorrem nos tribunais. "Os advogados vão tentar, mesmo nos casos de trânsito em julgado, invocar uma inconstitucionalidade." De resto, isso já foi feito em alguns processos.

"Eu não tenho esse entendimento e parece-me que o TC também não se pronuncia num sentido de a sua decisão afetar os casos transitados em julgado", sublinha Adão Carvalho.

Certo é, segundo o magistrado, que os advogados, seja de cidadãos já condenados, ou de cidadãos ainda em julgamento, vão tentar aproveitar esta situação para que ela jogue a favor dos seus clientes.

O que se segue?

O presidente do SMMP afirma que, "certamente, alvoroço vai acontecer". Para Adão Carvalho podem estar em causa litígios constitucionais: é que, se por um lado não é constitucional saber os dados dos cidadãos, também será inconstitucional fazê-lo só para alguns grupos.

"É uma questão de tentar encontrar soluções em termos legislativos que não são fáceis. A forma como o TC aborda o artigo 4.° torna quase impossível que se consiga coadunar com os fundamentos da inconstitucionalidade", conclui.

Fonte **CNN PORTUGAL**
Fotos **FREEPIK**

PROTEÇÃO DE DADOS

MUNICÍPIOS CONSIDERAM LEI DA PROTEÇÃO DE DADOS COMPLEXA E DE DIFÍCIL APLICAÇÃO

Lusa

Municípios contactados pela Lusa consideram que o novo regulamento de proteção de dados é complexo. Há dificuldades de aplicação nas autarquias, sobretudo nas mais pequenas, quatro anos depois da sua entrada em funcionamento.

O Regulamento Geral sobre a Proteção de Dados (RGPD), aplicado em Portugal e na União Europeia desde 25 de Maio de 2018, estabelece regras sobre privacidade e a proteção dos dados pessoais que as instituições públicas, incluindo autarquias, e privadas da União Europeia guardam dos cidadãos. E prevê que tenham um Encarregado de Proteção de Dados (EPD), uma espécie de "provedor" dos titulares dos dados.

Em declarações à Lusa, Carlos Pinto de Sá, presidente da Câmara de Évora (CDU), onde o RGPD ainda se encontra "em fase de implementação", considerou que a legislação "não olhou para a realidade" dos municípios e que, por isso, "apresenta dificuldades muito significativas de aplicação". Até agora, este município tomou um conjunto de medidas, como o facto de os dirigentes terem de "garantir a proteção de dados ao nível do seu serviço."

No entender daquele autarca, "vai ter que ter algumas alterações para ser eficaz"."Há um conjunto de questões que a legislação coloca que os municípios pequenos têm muita dificuldade em responder", argumentou, aludindo à nomeação de um EPD. Évora ainda não nomeou um EPD, mas Pinto de Sá adiantou que está a ser discutida na Comunidade Intermunicipal do Alentejo Central a possibilidade de existir "uma figura comum a vários municípios".

Consciente dos "desafios" que a alteração colocava, a Câmara do Porto constituiu, em 2017, um grupo de trabalho para dar cumprimento ao regulamento, tendo em 2018 criado um Departamento Municipal de Proteção de Dados, cujo principal propósito é "alertar e aconselhar" para o cumprimento das normas. Também nesse ano, o presidente da Câmara do Porto, o independente Rui Moreira, designou uma Encarregada da Proteção de Dados.

A densidade e complexidade do regulamento e a necessidade reforçada de formação dos colaboradores são desafios apontados pelo Porto. E pela Câmara de Coimbra (coligação liderada pelo PSD), onde o regulamento tem sido aplicado desde a sua criação, incluindo um EPD desde 2018.

A Câmara de Coimbra admite que a aplicação do regulamento "exige um esforço adicional e significativo". Exemplo disso é a

desmaterialização de processos nos serviços camarários, que têm levado à "alteração de procedimentos e de fluxos de circulação de informação".

A Câmara de Vila Real (PS), que nomeou o seu EPD em Março de 2021, assegurou que o software de gestão utilizado por este município "está preparado para responder às exigências do RGPD", estando "ativos os requisitos mínimos para cumprimento do previsto na lei". No entanto, referiu que ainda não foram elaborados os documentos do RGPD e da cibersegurança do município, "pelo facto de a responsabilidade da sua preparação ser da Comunidade Intermunicipal do Douro, para permitir a sua configuração no sistema de gestão".

sanções, afirmaram as autarquias.

Segundo o regulamento, os cidadãos têm de dar consentimento explícito para os seus dados pessoais serem usados – e para que fim – e podem pedir para sejam apagados a qualquer momento. A lei estabelece que a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional para efeitos do RGPD e que o incumprimento destas regras pode levar a sanções que podem ir, nos casos mais graves, até 20 milhões de euros e, nos casos menos graves de violação dos dados pessoais, até 10 milhões de euros.

O município de Lisboa designou o seu EPD após, em Junho de 2021, ter ocorrido uma polémica acerca da divulgação, por esta

Fonte da Câmara de Viseu (PSD) disse à Lusa que se encontra "em fase avançada o procedimento que permite a introdução no município deste regulamento". "Vai ser feita uma contratação exterior para colocar o regulamento em marcha. A figura do Encarregado da Proteção de Dados também será contratada nesse procedimento", acrescentou a mesma fonte, sem apontar uma data.

No Funchal (PSD), a principal câmara municipal da Região Autónoma da Madeira, o RGPD foi implementado em 2020, incluindo a designação de um EPD, e "tem decorrido dentro da normalidade", informou a autarquia. O executivo considera que, apesar de alguns problemas relacionados com a formação e sensibilização para esta temática, "até à data, tem sido possível responder a todas as situações no âmbito do RGPD".

No Funchal, no Porto e em Coimbra já houve queixas de cidadãos sobre o tratamento dos respetivos dados. Em pouco número e "sem provimento", pelo que não foram aplicadas

câmara, à embaixada da Rússia, de dados pessoais de activistas dissidentes russos, que na altura argumentaram que desta forma foi posta em causa a respectiva segurança e de familiares. Neste caso, a CNPD multou a Câmara de Lisboa em 1,2 milhões de euros por incumprimento do RGPD.

Em Setúbal, o presidente da Câmara, André Martins (CDU), nomeou um encarregado da proteção de dados no passado dia 3 de Maio, na sequência da polémica em torno do acolhimento de refugiados ucranianos no município sadino por cidadãos russos, alegadamente com ligações ao Kremlin. A CNPD abriu um inquérito à Câmara de Setúbal para perceber se houve ilegalidades no tratamento dos dados de refugiados ucranianos acolhidos, além de estarem em curso investigações da responsabilidade da Inspecção-Geral das Finanças e do Ministério Público.

Fotos **FREEPIK, CM SETÚBAL**

CIBERSEGURANÇA

MULTINACIONAL AMERICANA FORTINET INSTALA-SE NO POLITÉCNICO DA GUARDA

A Fortinet, um gigante mundial da informática, vai formar especialistas em cibersegurança no IPG, tornando-o assim num dos primeiros parceiros em Portugal a integrar o programa "Academia Fortinet".

Esta multinacional de informática, um gigante mundial na área da cibersegurança com sede mundial na Califórnia, vai instalar-se no Instituto Politécnico da Guarda – IPG, anunciou hoje o seu presidente, Joaquim Brigas, na sessão de abertura das Jornadas de Engenharia Informática de 2022 realizadas naquela instituição de ensino superior.

"Quanto à Fortinet, o Politécnico da Guarda estabeleceu recentemente uma parceria com este gigante da cibersegurança, tornando-se assim um dos primeiros parceiros em Portugal a integrar o programa 'Academia Fortinet'", afirmou Joaquim Brigas. "O Politécnico da Guarda irá formar especialistas na área de cibersegurança, aumentando a sua presença nesta área com grande procura de mercado!"

O anúncio foi feito na abertura das Jornadas de Engenharia Informática de 2022, as quais decorrem ao longo do dia 4 de maio, com um conjunto notável de palestras sobre cibersegurança, Internet das Coisas, Low Code, desenvolvimento na Cloud. As jornadas foram concluídas com uma mesa-redonda formada por quatro empresas que discutiram com a audiência questões relacionadas com projetos e tecnologias usadas e gestão de carreiras.

A iniciativa é organizada anualmente pelo Núcleo de Engenharia de Informática e pela unidade técnico-científica de Informática do IPG e terá como oradores representantes da Capgemini, Softinsa, Noesis, Merkle, Armis, Bosch, Fortinet, NTT Data, Loba, Magma e TRH.

"As Jornadas de Engenharia de Informática já são organizadas há mais de 18 anos. É uma tradição que permite aproximar os estudantes de informática das empresas tecnológicas e das tendências do mercado de trabalho", afirma José Fonseca, diretor de curso de Engenharia Informática e um dos organizadores desta iniciativa. "Preparámos um dia dedicado às novas Tecnologias de Informação e Comunicação com representantes de 11 tecnológicas de referência e parcerias do IPG".

Recorde-se que nas últimas semanas o IPG passou a acolher nas suas instalações os novos escritórios da consultora tecnológica portuguesa Noesis: a empresa compromete-se a recrutar recém-licenciados e mestrados no IPG para estágios, estudantes esses que, posteriormente, poderão prosseguir as suas carreiras na empresa. "Ter no Politécnico da Guarda uma consultora de referência do mercado como a Noesis, com uma elevada capacidade de inovação tecnológica, aproxima os nossos estudantes do mundo empresarial e promove a retenção de talento no Interior", afirmou o presidente do IPG.

Avançar para uma unidade de investigação na área da Informática

Na mesma sessão de abertura Joaquim Brigas apelou aos recursos humanos da área da informática para "ambicionarem uma unidade de investigação na área da Informática". Segundo ele, a prioridade dada pelo IPG à engenharia informática "irá seguramente atrair nómadas digitais, os quais poderão escolher a região da Guarda para trabalhar remotamente, beneficiando da sua qualidade de vida e aumentando o rendimento disponível das suas famílias".A presidência do IPG tem procurado dar às suas escolas condições, ambiente e meios para que elas associem a formação dos estudantes e a qualificação da mão de obra regional, com transferência de tecnologia e com uma ligação crescente do Politécnico às empresas e ao mercado. "A inovação empresarial é um fator de competitividade que é chave, não só para as empresas, mas também para as instituições de ensino superior como o Politécnico da Guarda", afirmou.

Fonte **POLITÉCNICO GUARDA**
Fotos **POLITÉCNICO GUARDA**

CIBERSEGURANÇA

COMPLEXIDADE DA REGULAÇÃO NA CIBERSEGURANÇA

Luís Avilez
(Consulting Cybersecurity Manager na EY)

A regulação é essencial para o cumprimento de metas de crescimento sustentável, promovendo o funcionamento correto de economias e sociedades. É esta que suporta a competitividade e equilíbrio dos mercados, protege os direitos e a segurança dos cidadãos e contribui para uma distribuição mais eficiente de bens e serviços. No entanto, apesar dos seus benefícios, a regulação não é isenta de custos. Como tal, é essencial a adoção de abordagens que otimizem os benefícios face aos custos e a implementação de mecanismos de monitorização.

Na cibersegurança, têm sido múltiplos os instrumentos a ser adotados pelos estados-membros da União Europeia com o intuito de aumentar a segurança e resiliência dos sistemas. Da Diretiva 2016/1148, da segurança das redes e da informação (SIR), à regulação no domínio do tratamento de dados pessoais e em outros, são múltiplos os exemplos da tendência acumulativa e fragmentária no quadro normativo.

Os desafios da regulação

Para as organizações, os custos da regulação podem contribuir negativamente para a competitividade. O investimento realizado na familiarização, gestão, monitorização, reporte, e formação dos quadros desviam recursos ao negócio e geram custos de oportunidade.

Para as organizações, a identificação dos requisitos associados à regulação pode ser um grande desafio, em particular para as que operam em múltiplas jurisdições. Noutras situações, as regulações podem requerer o reporte da conformidade e impor penalizações severas, incluindo a perda de licença, se não forem realizados de forma correta e atempada. A acumulação e fragmentação do quadro regulatório e as especificidades para alguns setores podem ainda somar maior complexidade.

Luís Avilez fala dos desafios atuais, da perceção das empresas e das perspetivas futuras da regulação no setor da cibersegurança.

A navegação num meio regulatório fragmentado e tendencialmente mais exigente é um dos maiores desafios atuais para os Chief Information Security Officer

Segundo o EY Global Information Security Survey 2021

O balanço que as organizações fazem

A COVID-19 trouxe um aumento substancial no volume de ciberataques, despertando uma maior sensibilidade do público em torno da cibersegurança e da atuação das autoridades. De acordo com dados do relatório da EY Global Information Security Survey 2021 (GISS)1, a navegação num meio regulató-

> ***Os CISOs estão menos confiantes de que a conformidade possa continuar a ser um fator que contribua para a melhoria dos níveis de segurança***
>
> *Luís Avilez*

rio fragmentado e tendencialmente mais exigente é um dos maiores desafios atuais para os Chief Information Security Officer (CISOs).

Dados do GISS alertam para que 1 em cada 2 inquiridos afirma que a conformidade pode ser um dos fatores de maior ansiedade na sua função. Com algumas organizações sujeitas a uma carga adicional de regulação específica setorial, a regulação pode, em algumas circunstâncias, exigir uma disponibilidade que os CISOs afirmam não dispor.

Perspetivas sobre o futuro

Em termos comparativos, em 2020, 46% dos inquiridos considerava que a regulação inspirava comportamentos positivos nas organizações. Com o aumento da complexidade regulatória, este número tem vindo a diminuir, situando-se atualmente nos 35%. Esta tendência anuncia que os CISOs estão menos confiantes de que a conformidade possa continuar a ser um fator que contribua para a melhoria dos níveis de segurança.

Seis em cada dez inquiridos consideram que a regulação se tornará mais heterogénea e que consumirá mais tempo, tornando-se cada vez mais um fator de distração.

Atenuar os custos da regulação

Através da adoção de uma abordagem estruturada, as organizações podem reduzir substancialmente o esforço associado à conformidade. Organizações que operem com diferentes regulações deverão dar prioridade à elaboração de um programa global de políticas e controlos que se adeque aos aspetos comuns, realizando posteriormente adendas específicas para tratar das exceções.

Outro fator de sucesso é a adequação de processos e de tecnologias. A identificação incorreta de requisitos para avaliação das soluções tecnológicas ou o desenho de processos ineficientes podem traduzir-se em custos elevados de conformidade. Processos e tecnologias devem ser avaliados por equipas com experiência.

Num contexto regulatório cada vez mais exigente, processos de conformidade pouco eficientes podem facilmente resultar em custos elevados e são um fator de desmotivação dos melhores quadros, já de si escassos na cibersegurança.

Fonte **ECO, EY**
Fotos **EY.COM, FREEPIK**

CIBERSEGURANÇA

MODELO DE GOVERNO PARA A CIBERSEGURANÇA

Rodrigo de Perez Monteiro
(Technology Consulting Cybersecurity Manager na EY)

As empresas que estão hoje a implementar ou a robustecer os seus programas de cibersegurança, só o vão conseguir fazer com sucesso se tiverem um modelo de governo bem definido e uma gestão do risco eficaz.

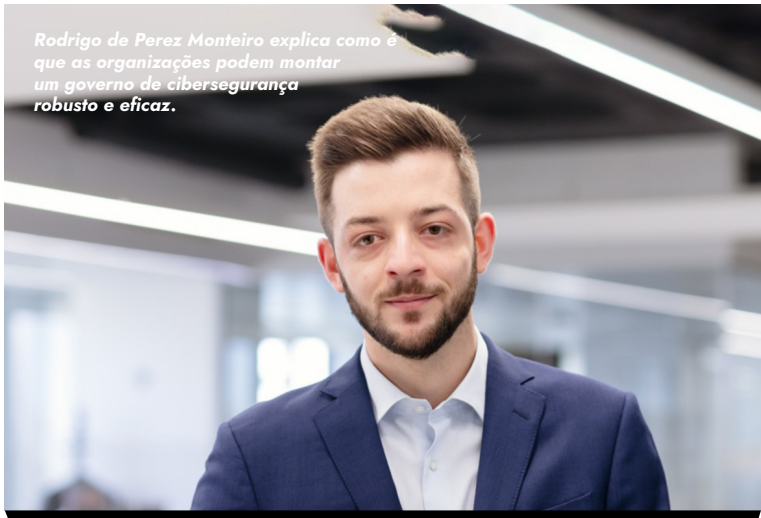
Como definido no primeiro princípio do modelo das três linhas proposto pelo IIA (The Institute of Internal Auditors), atualizado recentemente, o governo de uma organização necessita das estruturas e processos apropriados que permitam:

- Definir os responsáveis últimos para a supervisão através da integridade, liderança e transparência;
- Definir as ações de gestão para atingir os objetivos da empresa através de tomadas de decisão com base no risco;
- Garantir a independência das funções de auditoria interna de forma a dar confiança e facilitar a melhoria contínua dos processos.

A Responsabilidade Social Corporativa (RSC) veio contribuir para que a adoção de modelos de governo seja cada vez mais uma realidade nas empresas, através do critério de Governo Corporativo (ao qual se juntam também os critérios Ambiental e de Sustentabilidade – ASG).

A fim de implementar um modelo de governo holístico para a cibersegurança, as organizações devem conciliar a dimensão dos esforços com a sua capacidade interna, podendo recorrer a parceiros que os apoiem. Para o efeito, sugere-se a adoção de uma abordagem faseada, que passa por:

1. Criar uma cultura de cibersegurança, assente numa estratégia e visão a longo prazo, com definição e comunicação clara de papéis e responsabilidades, que capacite todos os elementos da organização para a proteção da confidencialidade, integridade e disponibilidade dos seus ativos de informação. De sublinhar que o Chief Information Security Officer (CISO)



Rodrigo de Perez Monteiro explica como é que as organizações podem montar um governo de cibersegurança robusto e eficaz.

O governo eficaz da cibersegurança permite que as organizações maximizem os benefícios de operar numa economia digital, apoiando a sustentabilidade do negócio.
Rodrigo de Perez Monteiro

deve desempenhar um papel chave no governo da cibersegurança da organização. Não obstante, deve ser considerada a criação de um comité de cibersegurança, que acompanhe as iniciativas em curso, garanta a adequada alocação de recursos financeiros, humanos e tecnológicos, e consiga o buy-in de todas as partes, poderá ser um contributo determinante para a execução da estratégia. A formalização destes elementos

deverá ser feita através duma framework documental de políticas e procedimentos, alinhada com as boas práticas de segurança de informação de referenciais normativos, como a ISO/IEC 27001:2013.

2. Alinhar a gestão do risco de cibersegurança com os modelos de gestão de risco corporativo presentes na organização. A adoção de uma framework formal de gestão de risco potenciará a produção de resultados consistentes e repetíveis. Ao usar um padrão estabelecido como a ISO 27005:2018 ou NIST SP 800-30r1, a organização pode avaliar ameaças, vulnerabilidades e impactos dos riscos de segurança no contexto do seu negócio, bem como estabelecer métodos adequados para mitigar os riscos. A gestão adequada do risco apoia a tomada de decisão, maximizando o benefício do investimento em cibersegurança.

3. Estabelecer um programa de cibersegurança, que traduza a estratégia em ação, impulsionando iniciativas e melhoria contínua da ciber-resiliência. As iniciativas do programa devem incluir itens como formação/sensibilização, desenvolvimento de políticas/procedimentos, implementação de novos sistemas/ferramentas de segurança ou a gestão do ciclo de vida das tecnologias implementadas.

4. Medir e reportar a capacidade de ciber-resiliência da organização, que resulta da execução do programa de cibersegurança. Os relatórios a produzir devem proporcionar às partes interessadas uma garantia de que a organização é ciber-resiliente, documentar o retorno do investimento (ROI) em iniciativas de cibersegurança e promover a melhoria contínua. Para o efeito, a organização deverá definir SMART* KPIs (quantitativos ou qualitativos) que forneçam insights sobre tendências, riscos e comportamentos, bem como destacar necessidades de mudanças na estratégia, gestão do risco, ou política de investimento.

O governo eficaz da cibersegurança permite que as organizações maximizem os benefícios de operar numa economia digital, apoiando a sustentabilidade do negócio. Sem um governo correto da cibersegurança, as organizações terão cada vez mais dificuldade em assegurar a continuidade das suas operações ou manter a confiança dos stakeholders externos (clientes e parceiros), com os impactos financeiros, reputacionais, e outros daí decorrentes, pelo que esta deve ser encarada como uma prioridade, pela gestão.

** SMART model: Specific, Measurable, Achievable, Relevant, and Time-bound (Específico, Mensurável, Alcançável, Relevante e Limitado no Tempo).*

Politécnico de Viseu
Politécnico da Guarda
ipvc Instituto Politécnico de Viana do Castelo
Cofinanciado por: COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

CIBERSEGURANÇA: A SUA CAIXA DE CIBERFERRAMENTAS

[direcionado aos cidadãos]

Com o objetivo de aumentar a resiliência do ciberespaço de interesse nacional, o Centro Nacional de Cibersegurança encoraja todos os cidadãos a adotarem as melhores práticas de cibersegurança, recorrendo a esta caixa de ferramentas de boas práticas prontas a usar.

7 Boas Práticas prontas a usar

As boas práticas descritas neste documento não seguem uma ordem específica. Os cidadãos devem adotar as mesmas de acordo com as suas necessidades.

Ativação da Autenticação Multifator (MFA)

Proteja-se utilizando mais do que um fator de autenticação quando acede às suas contas (por exemplo, banco online, pagamentos online, redes sociais, email e outras plataformas online).

Gestão de Palavras-Passe

Mantenha as suas palavras-passe secretas e seguras (use uma frase com 12 caracteres ou mais, sem termos óbvios), evitando que alguém, com intenções maliciosas, aceda às sua plataformas protegidas com palavras-passe.

Phishing

Não clique em links ou anexos de emails e SMS suspeitos, nem partilhe os seus dados em resposta a essas mensagens.

Atualização de Software

Garanta que o seu software se encontra devidamente atualizado.

"NÃO" à Desinformação

Assegure-se de que as notícias qu
e lê são veiculadas por fontes fidedignas e não partilhe conteúdos que não sejam de plataformas de confiança.

Uso de Antivírus

Proteja os seus dispositivos contra o malware com a instalação apropriada de um antivírus.

Uso de Firewall

Faça da firewall a sua "parede de fogo" de modo a bloquear o acesso não autorizado às suas redes privadas.

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

https://www.cncs.gov.pt/