7.ª edição da C-Days (2021) "Naturalizar competências"

CONCLUSÕES

15 de junho de 2021

A C-DAYS é uma conferência organizada anualmente pelo Centro Nacional de Cibersegurança (CNCS), com o objetivo de promover o debate em torno da temática da cibersegurança.

A conferência C-DAYS de 2021, a sua 7.ª edição, é dedicada às competências em cibersegurança e à ***necessidade de as tornar comuns entre as pessoas e as organizações.***

"Naturalizar competências" é o mote da edição deste ano, para se tomar consciência do que fazemos com os nossos dados nos planos pessoal e profissional. Nesta fase, "proteger as estruturas administrativas é uma prioridade", diz-nos **Miguel Pereira Leite, Presidente da Assembleia Municipal do Porto**, que reconhece a necessidade de investimento nas infraestruturas digitais e no conhecimento para prevenir situações de imprevisto.

Miguel Pereira Leite diz que o Porto está a privilegiar empresas que criem quadros altamente qualificados em cibersegurança. **Na cidade, já se aposta em empresas que sejam fiáveis e que tenham uma política interna de proteção de dados que permita utilizá-los com maior eficiência, assentes em plataformas de dados abertos, elevando a transparência e cidadania ativa e contribuindo para gerar mais valores.**

No Porto há já vários serviços que recorrem à inteligência digital, sendo exemplos disso o plano de gestão de resíduos, desenvolvido pela Porto Ambiente, e a equipa de proteção civil que também controla a meteorologia com contributos vindos, igualmente, dos cidadãos.

Nestes três dias vão ser debatidos vários temas relacionados com cibersegurança em várias dimensões, como sociedade, riscos e conflitos, ética, economia, inovação e políticas públicas.

Lino Santos, Coordenador do Centro Nacional de Cibersegurança (CNCS), recorda que no ano passado, mais de oito mil pessoas acompanharam este evento que se realizou em Cascais, mas, devido aos constrangimentos causados pela pandemia, foi, igualmente, transmitido online.

O coordenador do CNCS deu o alerta para a importância deste tema, através de exemplos de crises de cibersegurança internacionais geradas com o recente ataque de ransomware à Colonial Pipeline e o ciberataque de ransomware ao sistema nacional de saúde irlandês – tudo aconteceu já em 2021.

O volume deste tipo de incidentes quase duplicou no ano passado, coincidindo com os períodos de maior teletrabalho – fraude, burla, phishing e ransomware são os mais comuns. Tudo isto requer uma forte aposta na criação de competências para pessoas e organizações em cibersegurança.

Tornar essas competências inatas e alcançar a imunidade de grupo nesta área é o que o CNCS pretende alcançar a curto prazo.

Mariana Vieira da Silva, a Ministra do Estado e da Presidência, enviou um vídeo, marcando, assim, presença neste primeiro dia de três C-DAYS.

"Naturalizar competências" considera ser um bom mote porque **as queixas apresentadas no ano passado aumentaram 182% e estes ataques paralisam sistemas públicos, causando profundas perturbações à sociedade.**

No seu entender o futuro passa por "capacitar pessoas para uma vida cada vez mais digital e para desenvolverem competências em cibersegurança".

Portugal tem uma estratégia nacional de segurança no ciberespaço que passa por ações de sensibilização, mas que precisa de ser aprofundada; são necessários mais e melhores profissionais nesta área para promoverem a resiliência digital. "O Estado criou condições para o desenvolvimento dessas competências e reforço da comunicação nesta área. A agenda europeia de cibersegurança é apoiada por redes nacionais que Portugal privilegia muito", acrescenta a ministra.

Entretanto, está a ser criada uma academia de cibersegurança para trabalhadores de organismos da administração pública. Os Digital Innovation Hubs e a criação de selos de cibersegurança são exemplos de iniciativas já criadas na sequência do PRR – Plano de Recuperação e Resiliência.

A nova estratégia europeia para a cibersegurança aumenta a necessidade de se dar uma resposta conjunta no sentido de se promover a resiliência, a soberania tecnológica e reforçar a promoção de um ciberespaço aberto em segurança e com capacidade de reação pronta.

Mariana Vieira da Silva finalizou a sua intervenção a considerar que o desenvolvimento de competências tem de passar por toda a sociedade e ocupar um lugar ao longo da vida em todas as formações.

António de Sousa Pereira, Reitor da Universidade do Porto, fez uma apresentação assente no paralelismo dos 10 mil triliões de grãos de areia existentes no Planeta, à possibilidade, desenvolvida mais à frente, de se encherem 10 mil triliões de *pens* de um giga com dados.

O reitor nota que tem havido um incremento brutal na capacidade de armazenar informação, pelo que o domínio nesta matéria é absolutamente crítico. Há grandes bases que acumulam dados e as que os partilham ainda são maiores porque vão gerando informação.

Quando analisamos o volume de informação digital sobre o qual podemos trabalhar para chegarmos a algoritmos, estamos a trabalhar em informação digital que cresce brutalmente. A projeção num futuro próximo aponta que em 2029 acumulamos informação digital que ocupará 10 mil triliões de gigabites. "É sobre este volume de informação que tem de se encontrar algoritmos que possam explicar vida, arte, música e, em suma, o Universo. Quem faz *data mining* quer discutir com Deus a formação do Universo e as leis que regulamentam tudo o que nos acontece", reflete António de Sousa Pereira.

Em seguida, o reitor cita Alan Touring para dizer que os fenómenos complexos têm uma explicação matemática. Como exemplo refere o ADN humano que está assente em quatro variáveis que se conjugam e alternam umas com as outras, permitindo assim inúmeras variações.

Muito do trabalho atual passa por compreender as regras básicas da Ciência que converge para um dogma segundo o qual os organismos são algoritmos e a vida nada mais é que processamento de dados. A evolução constante vai levar à criação de máquinas cujos comportamentos não se distinguem dos comportamentos humanos.

Isto cria um **problema ético – a divergência entre inteligência e consciência** que traz muitos riscos para a sociedade, adverte.

Mas nem tudo tem uma visão tão trágica para o reitor. No campo da saúde, constatou-se que os nanomotores moleculares poderão condicionar a morte (que pode ser considerada uma doença). Para que tal aconteça, tem que se garantir que as topomerases replicam o ADN sem defeitos e poderão, deste modo, prolongar em muitos anos a vida humana. Testes já feitos em laboratório confirmam-no numa triplicação da vida de pequenos animais. O futuro, auspicioso, passa por estudar e replicar o que tem o ADN das pessoas que vivem mais de uma centena de anos.

Debate – 1.º painel

Pedro Inácio, Professor da Universidade da Beira Interior, começa por referir que os *devices* que estão na nossa vida 24 horas por dia / 7 dias por semana são os que mais nos deveriam preocupar à data de hoje. Acredita que vai ser natural o Security By Design e que, um dia, ninguém tenha que se preocupar com cibersegurança por esta estar assumida à partida. Mas isto talvez ainda demore mais de 50 anos a acontecer, considera o professor: "As pessoas dão as suas passwords, as mesmas são fracas, acreditam em qualquer e-mail que recebem. Há um conjunto de atores que põem em causa a confiança original e o fator humano de base é o da confiança".

Requisito inicial para se trabalhar em cibersegurança é a capacidade para aprender ao longo da vida. Depois, tem de ser alguém engenhoso, que queira "pôr as mãos na massa", não ter uma atitude arrogante, ter capacidade de antecipação aos problemas e não ter medo de errar nem de admitir que errou.

As universidades estarão a formar em competências-chave? "Sim, há estudantes que querem fazer trabalhos em cibersegurança e há cursos com, pelo menos, uma unidade curricular em cibersegurança".

Se quisermos um bom profissional de cibersegurança, tem que lhe ser dada a perspetiva; o caminho que o hacker segue. Os atacantes pensam de forma

"extraterrestre" e é necessário entrar nas suas cabeças para perceber que labirintos percorrem até cumprirem com as suas intenções.

A educação em cibersegurança deve começar pelos mais pequenos, nem que seja no estabelecer da diferença entre o que é bom e o que é mau. Os mais jovens gostam do tema e conseguem criar **um movimento de "arrastamento**" entre colegas e familiares. Análise crítica é capaz de ser a melhor *skill* a desenvolver.

Luísa Ribeiro Lopes, coordenadora geral do InCode 2030, é da opinião que, no futuro, é preciso naturalizar estas competências digitais de que se estão a falar; é preciso adaptar, dar poder a quem tem competências digitais e dentro delas criar capacitação em cibersegurança – só assim há capacitação no digital.

"Todos temos que ter noções básicas de cibersegurança, além de competências digitais", considera.

Exemplo do que está a ser feito para dotar os cidadãos destas novas competências é o curso de cidadão ciberseguro que foi o mais frequentado feito na plataforma NAU em 2021, de onde se conclui que as pessoas estão interessadas em saber como podem estar mais seguras.

Educação e formação são áreas essenciais e o trabalho está a começar pelos mais jovens. Deverá seguir-se a requalificação dos trabalhadores e da população ativa que têm uma formação básica em cibersegurança.

Contudo, nesta busca por uma população mais cibersegura, é importante não esquecer que a exclusão social e económica tem reflexo no digital e é isso que tem de se combater. É preciso ir para o terreno: formar e capacitar, logo no ensino básico, secundário e superior, formando profissionais capazes de dar resposta ao mercado de trabalho.

Exercer a cidadania com pensamento crítico é o mais importante: ler, interpretar e optar entre fazer "a" ou "b". **Literacia digital é saber distinguir situações.**

Luís Vidigal, um dos fundadores da Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI), apresentou o mais recente estudo (https://apdsi.pt/produto/estudo-exploratorio-mapeamento-das-necessidades-de-competencias-na-area-das-tice-visando-o-ajuste-da-oferta-formativa/) da APDSI, do qual resultou que a maioria das 1500 empresas questionadas não têm a cibersegurança nas suas prioridades, apesar de reconhecerem a sua importância. Uma certificação de alto nível em cibersegurança pode custar até seis mil euros por semana, e a verdade é que a maioria não tem hipótese de fazer um investimento financeiro tão avolumado. **O estudo concluiu que há uma grande fragilidade na perceção da necessidade da aposta em cibersegurança.**

Atualmente há uma duplicação constante dos dados. A cada 11 dias duplica o conhecimento e a tendência é para este prazo encurtar. Tudo acontece a uma velocidade vertiginosa e já não são humanos a criar e resolver problemas. O futuro é, portanto, incerto.

O sistema formal tem que apostar fortemente na cibersegurança, mas é preciso que as pessoas também **aceitem a formação ao longo da vida**; terem muita curiosidade sobre o assunto é fundamental.

Mais do que ter poder é preciso ter autoridade e credibilidade assente em conhecimento – que neste domínio, perde atualidade quase diariamente.

Ethical hackers serão a solução ou podemos trazer os cibercriminosos para o lado do bem? "O ethical hacker pode perder algum entusiasmo inicial. Esta é uma área muito desafiante", considera Luís Vidigal. O framework de competências tem de ser dinâmico, como dinâmica é esta área. Há áreas como a banca e a saúde que já têm muita experiência. Na área forense, a título de exemplo, há 85% de ciberataques.

O *Security by Design* tem de ser levado ainda mais a sério na criação dos sistemas que, mais do que seguros, **devem ser auditáveis pelo próprio**; a empresa tem o direito de saber o que está a ser feito com os seus dados. Este sistema também tem de envolver o mercado e as empresas, mas é uma área de soberania; a estratégia de segurança não pode ser sujeita a outsourcing ou subcontratados.

Por fim, Luís Vidigal adverte que as competências técnicas têm que ser acompanhadas por competências humanas. Se a pessoa não tem uma estrutura de valores capaz, pode ser um "profissional" perigoso.

Soft Skills necessárias para um profissional de cibersegurança: ser determinado, colaborativo, querer aprender e ser curioso, analítico, perspicaz e pensar de forma hipercrítica permanentemente.

Joana Alvarez, do CNCS, pega na questão da autoridade que é dada pelo conhecimento reconhecido, certificado e que antecipa necessidades futuras. Esta é a base do **referencial de Singapura em competências de cibersegurança que valoriza a importância do fator humano. A tecnologia é feita e usada por humanos, por isso, o mapeamento de competências em cibersegurança tem de ir buscar várias linhas e passar pelo diálogo entre vários agentes.**

Este é um referencial para a implementação do ciclo de vida da gestão da Cibersegurança de uma organização, tendo em atenção os aspetos humanos, tecnológicos e processuais, com especial foco nos processos e procedimentos da gestão do risco. Ainda assim, na cibersegurança estão em causa competências humanas e é preciso trazer profissionais também de fora do conhecimento técnico, como filósofos, politólogos e sociólogos.

Referenciais de competências devem ser dinâmicos e não estáticos porque a própria área é mutável e sujeita a tendências. Há competências básicas em cibersegurança, contudo, que têm de estar sempre garantidas.

Os conhecimentos nesta área devem estar certificados por uma academia com autoridade, sublinha Joana Alvarez. O fator humano é fundamental para gerar confiança e rigor que também se fazem através da certificação / conhecimentos selados.

Outra *soft skill* importante do profissional de cibersegurança é a empatia.

Debate – 2.º painel

O segundo painel contou com o contributo de Carlos Neto, Professor da Faculdade de Motricidade Humana (FMH) da Universidade de Lisboa (UL), para quem naturalizar competências é uma tarefa complexa, mas transversal. Temos que pensar na escola, família e comunidade. Que escola temos e teremos no futuro? **A velocidade da transição digital acontece muito rapidamente e o digital tem que ser visto como uma literacia.**

"Há uma grande percentagem de jovens muito sedentários, houve uma explosão de tempo passado no ecrã agravada pela pandemia. O risco também é digital, mas temos que tentar dominar a situação e não ser dominada por ela. Não se atiram para o digital, crianças sem conhecimentos prévios, como não se atira uma criança para uma piscina sem saber nadar", diz.

O cérebro não vive sem um corpo, portanto, estes desafios para o digital passam por formação para pensamento crítico para um mundo incerto e desconhecido. É possível que estas crianças tenham capacidade para resolver problemas complexos e saberem comunicar. Devem ter, todavia, uma preparação para saberem lidar com o risco digital e o risco possível.

Esta naturalização deve respeitar a idade das crianças a quem a formação se destina, por isso, deveria haver um conjunto de *guidelines* que ajudem pais e professores para que as crianças consigam ter algumas capacidades para enfrentar os perigos que existem no ciberespaço; todos temos que aprender – até os adultos.

Não é possível as escolas seguirem o mesmo modelo de aprendizagem de há 50 anos; os professores têm de gerir bem e com muito cuidado a "escravização digital" consciente que estamos a seguir. Tem havido uma enorme redução de competências lúdicas e motoras na adolescência, afirma o professor: **"estamos a criar crianças analfabetas motoras. Não sabem atar os sapatos, mas sabem mexer em iPads".**

Os professores devem ser "guias críticos" para ajudarem as crianças e jovens; é preciso requalificar a escola com outros currículos.

Só há segurança se houver ameaça de risco, mas a preocupação também deve ser em naturalizar e humanizar as novas tecnologias. Crianças hiperativas são as que estão sentadas no sofá, que não se mexem. Só se olha para o cérebro, para uma parte do problema, e não para o corpo todo.

Cristina Ponte, Professora da NOVAFCSH (Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa), começa por enquadrar que estas preocupações com crianças e jovens na Internet e com ameaças de pessoas com más intenções já é antiga, mas agora a preocupação foca-se também no *ciberbullying* e este assunto foi trazido por crianças e adolescentes que o reportavam. Daí **a necessidade de se ouvirem os mais jovens sobre a sua experiência no digital.** Hoje, há mais oportunidades, mas também mais riscos que derivam da intensificação da experiência no digital. **Hoje estamos em contacto permanente com o online e vive-se um capitalismo sobre os nossos dados; somos quase forçados a dar os nossos dados.**

As crianças nascem e crescem no ambiente digital, mas não têm competências para lidar com isso. Muitas vezes antes de nascer, a criança já tem uma pegada digital que não pôde controlar.

Há necessidade de considerar formação de professores para o que são as crianças de hoje, que vivem num ambiente de estimulação constante; há uma ansiedade em fazer e cumprir com tudo o que é novo. **Normalmente, os adolescentes e jovens recorrem aos seus pares para obterem respostas, pelo que são eles que têm de ter também este protagonismo no sentido de serem orientadores e sensibilizadores para estas questões de segurança.**

Já existe a disciplina TIC no ensino básico e secundário. A importância do trabalho emocional e empatia ser capaz de perceber o que as crianças estão a ver nos ecrãs, a literacia digital tem de ser vista de forma integrada, com foco nos aspetos comunicacionais e criativos, e tudo isto tem de ser trabalhado por pais e professores.

No espaço Europeu também tem havido a preocupação de debater estes assuntos. O risco zero é não usar, mas esse também leva à exclusão. Tem é que se considerar o

menor risco possível e que todos possam usar a net para entretenimento e informação nas melhores condições. **A formação tem que ter foco na técnica, mas também nos aspetos sociais e criativos.**

Rosário Carmona e Costa, Psicóloga Clínica, tem-se debatido muito, em contexto clínico, com a questão de como educar os filhos nesta nova era. Não há uma solução mágica a não ser fazer o que sempre foi feito: "educar com base nos melhores valores e na inteligência emocional: educamo-los da mesma forma que queremos que se relacionem com os outros e educando para a empatia, tolerância, frustração, respeito pelo outro, proteção, assertividade, e o expressar de opiniões respeitando os outros. Fazer o equilíbrio entre fazer o que está na moda e conseguir uma definição de identidade, pode ser a solução".

Hoje há uma grande dicotomia nas escolas: há as que fazem um ensino muito apelativo; outras que, pelo contrário, apostam numa modalidade mais antiga. E será que as crianças aprendem melhor através das apps? Só se forem mediadas por um adulto, diz-nos.

É preciso que os mais jovens saibam lidar com a ansiedade, por exemplo, para não procurarem no online um escape para isso. **É preciso educar os adultos que educam os jovens.**

As plataformas de reporte de abuso devem ser acessíveis a todos; quando alguém passa por essa situação deve ter facilidade em reportar.

As empresas também têm a "obrigação" de fornecer ambientes seguros online e olhar para o risco como uma oportunidade – a de aprender a defender-se.

A psicóloga também é da opinião de que já chega de disciplinas nas escolas; é preciso, isso sim, saber como nos relacionarmos com as pessoas e o que se faz "quando não há nada para fazer".

Sofia Rasgado, do CNCS, coordena um projeto destinado a crianças. No seio deste projeto, os profissionais tentam adequar os recursos e a intervenção a cada um dos

targets específicos; já há essa preocupação de desenvolver recursos que vão, por exemplo, responder às necessidades dos seniores.

Em muitos assuntos, como este, são os mais jovens a formarem os pais.

O **Centro Internet Segura** tem dois polos de sensibilização. Ao CNCS cabe desenvolver recursos que explorem como lidar com os riscos e a forma como são diagnosticados. As sessões são dinamizadas em vários espaços (escolas ou associações) e ajudam as crianças e jovens a perceber como agir face a determinadas ameaças.

Há ainda a **linha Internet Segura** para esclarecimentos face à utilização da Internet e outra componente de denúncia de conteúdo ilegal. Até maio, chegaram queixas de 652 ameaças de cariz sexual online, o que corresponde a um aumento “explosivo”. A novidade ainda mais preocupante é que este tipo de conteúdo está a ser produzido pelos próprios jovens.

O CNCS também produz recursos que vão ao encontro de necessidades de todos os cidadãos porque “é importante desenvolvermos mecanismos de aprendizagem fora da escola”. Como naturalizar competências? A recomendação passa pelo regresso às origens, a um momento físico offline, para depois todos saberem estar expostos ao online.

É preciso saber dominar a cultura digital para não sermos dominados por ela, pelo que as crianças precisam de uma “pedagogia digital” diferente entre idades.

É preciso lidar com riscos, mas fruir das tecnologias. É preciso uma formação de professores e evitar uma escravização digital. Família, escolas, empresas, jovens, adultos e crianças – todos têm um papel. Os professores devem ser mediadores nestes novos processos de aprendizagem. Noutro prisma, empresas e políticas públicas também têm um papel.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e societais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, a Governação das TIC, a Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação e as Competências digitais.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt

email | secretariado@apdsi.pt

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Associação de Utilidade Pública

ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Patrocinadores Globais da APDSI

accenture aws Google