Conferência "Cibersegurança"
CONCLUSÕES

12 de julho de 2022

A APDSI fechou o primeiro semestre de atividades para 2022 com uma Conferência sobre Cibersegurança, a 12 de julho, na NOVA SBE.

Num mundo definitivamente digitalizado, estamos perante novos riscos e pontos de ação.

Para Governos, setor público e empresas, estes avanços traduzem-se numa constante ameaça que já foi visível em vários casos conhecidos de ciberataques em Portugal, como aconteceu à Vodafone PT e ao grupo IMPRESA. As seguradoras também estão cada vez mais implicadas nesta nova realidade.

Israel foi um dos casos trazidos à conferência, como exemplo de um ecossistema atento e ativo em segurança cibernética.

Helena Monteiro, Presidente da Direção da APDSI, recordou os MeetOns – as pequenas conferências à distância que a APDSI lançou em período COVID – e congratulou-se por esta conferência ter um formato híbrido. **Fez votos para que a reunião decorresse de**

forma agradável, apesar de o tema ser "aterrador", embora observando que esse **"terror"** se vai dissipando à medida que vamos ficando cada vez mais esclarecidos.

A Professora Helena Monteiro agradeceu à NOVA SBE – School of Business and Economics, na pessoa do seu Diretor, Daniel Traça, o apoio institucional dado ao evento, assim como o apoio dado pela sua equipa.

Agradeceu ainda ao conselheiro Eng.º Gonçalo Caseiro, por abraçar o tema da cibersegurança com a APDSI e ter apoiado a configuração da Conferência, e bem assim a todos os convidados que contribuíram com os seus "use cases", experiências e indicações sobre as práticas que seguiram e recomendam seguir.

Por fim, dedicou algumas palavras especiais ao Keynote Speaker Yigal Unna, ao Contra-almirante António Gameiro Marques por ter aceite encerrar a Conferência e ao Vogal da Direção da APDSI, Dr. Nuno Guerra Santos, a quem coube a coordenação da conferência.

Daniel Traça, Reitor da NOVA SBE - School of Business and Economics, explicou a importância que o tema tem para a universidade. Criar um espaço onde os alunos pensem no futuro, foi o desafio que os seus responsáveis transpuseram para um edifício no qual tudo é transparente, com vidros, onde qualquer cidadão pode entrar sem ter de se justificar a um vigilante e desfrutar de um espaço aberto à comunidade, que é um ponto de encontro entre pessoas e um espaço colaborativo para o desenvolvimento de novas e inovadoras soluções. "Este é o ambiente que faz pessoas e equipas produtivas e enche os alunos de esperança", acredita Daniel Traça.

Nos últimos tempos o campus da NOVA SBE, "uma escola de e para pessoas", tem registado um crescimento bastante significativo, com 1600 conferências realizadas num ano e 6% delas foram internacionais. **"É difícil fazer com que os seres humanos sejam criativos num ambiente de terror"**, diz o Reitor, que acredita que, apesar de haver um sentimento generalizado de medo que vai afetar a criatividade nas empresas, é muito importante trazer a cibersegurança para o *core* dos negócios, sendo esta **uma questão de estratégia e criação de cultura na organização.**

Sendo certo que as consequências dos problemas ligados à cibersegurança são para as pessoas, também são elas que as inspiram, através dos hábitos que vão ganhando.

É preciso, pois, trazer profissionais bem-sucedidos para o combate ao cibercrime, defende Daniel Traça: **“se matarem a cultura da empresa, a inovação e a capacidade de correr riscos, a vossa organização já perdeu. Os líderes têm de fazer investimentos, mas trazer ao de cima o sentimento de que todos são responsáveis pelos sucessos alcançados”**.

Cibercrime já é muito mais que *hacking*; hoje em dia há roubo de identidade e propriedade pela via digital e este será o tópico dominante das novas tecnologias para os próximos cinco ou seis anos. **As pessoas vão ter de ganhar o hábito de se defender do *hacking* e dos ataques, à medida que se vão “normalizar” entre nós.**

Yigal Unna, Israel National Cyber Directorate Former Chief, afirma que desde 1998 se fala nesta questão a que hoje em dia chamamos de cibersegurança e que nos últimos quatro anos lidou mais com o tema do que nos anteriores 29 a trabalhar nesta área, porque, na verdade, há 10 anos nenhum destes cuidados era necessário e nem fazia sentido haver uma preocupação redobrada com a proteção dos civis de ataques de cibersegurança.

“Ciber é tecnologia, sem dúvida, mas é mais sobre como ela pode ser usada e abusada em vários aspetos. E quando se entendem como esses abusos ocorrem, estamos num bom ponto para entender cibersegurança” refere **Y**igal Unna, que também vê nesta matéria possíveis oportunidades.

Há milhares de organizações, privadas e públicas, que já enfrentaram o terrível cenário de terem todos os seus ecrãs bloqueados sem saberem o que fazer nem como podem voltar a trabalhar. O *ransomware* faz das suas sem qualquer aviso e muitos têm sido os que fiquem presos a um ataque que parece sem solução.

O responsável israelita lembra que na Costa Rica, há cerca de dois meses, todos os sistemas do país tiveram um *lockdown* bastante preocupante, e na **“guerra na Ucrânia**

sabemos que este é um ponto de partida para qualquer novo conflito que surja; um problema que afeta o armamento e ainda acentua mais as crises humanitárias instaladas entre civis inocentes de ambos os lados”.

85% das atividades de cibercrime atualmente estão a acontecer na Ucrânia e os ataques estão cada vez piores. Se até aqui os *hackers* se dedicavam à espionagem, agora avançaram mesmo para a destruição total de dados e sistemas (agora são *wipers*). Durante um período tão conturbado como este, há muito trabalho para fazer e é preciso ter a noção, alerta Yigal Unna, que os próximos ataques por toda a Europa vão ser muito piores. Os ataques vão passar a ser uma infraestrutura tão crítica como é a democracia.

No ano passado, mais de 2200 ataques de *ransomware* foram registados diariamente, tirando partido de 43 grandes vulnerabilidades detetadas e provocando prejuízos na ordem dos cinco mil milhões de euros. Nos próximos tempos, **o mundo vai aperceber-se que a culpa da inflação tem a ver com os três mil milhões que estão a ser pagos em *ransomware* e que estão a fragilizar as economias.** É um problema global que atinge toda a gente e o seu combate tem de começar nas universidades.

Outro caso lembrado por Yigal é o do gasoduto americano Colonial Pipeline, em 2021. O ataque só atingiu a rede administrativa, onde 50 mil computadores ficaram comprometidos. Nas gasolineiras não se verificava qualquer anomalia, mas como o lado administrativo não funcionava, todo o processo estava comprometido.

Como não era possível controlar o que acontecia nos postos de abastecimento, as bombas começaram a secar e o caos instalou-se em cerca de duas semanas com os media a potenciarem todo o tipo de explosões humanas que podiam acontecer. Foi espalhado o alarme porque os cidadãos perderam a confiança numa rede de abastecimento de combustíveis que foi fortemente impactada com a situação. 45% dos serviços da Costa Este fecharam ou ficaram comprometidos durante o período mais crítico do ciberataque.

Ainda assim, não havendo forma de responsabilizar estes cibercriminosos, o número de detidos neste âmbito “é ridículo, é quase nada porque este é o crime perfeito que pode

acontecer a milhares de quilómetros de distância do seu autor. O resgate pode ser feito em criptomoedas, ou seja, sem deixar rasto”.

35% dos cibercrimes tiveram origem em Israel e como destino as instituições financeiras do Dubai. A polícia investigou e descobriu que eram todos bons cidadãos, sem cadastro, pagavam impostos e tinham os filhos nas escolas. Os que atacam Portugal não vivem aqui e muitas vezes nem perto, o que se torna num problema gigantesco. Os cidadãos comuns são o alvo, o estrago pode ser muito amplo.

Neste último ano, os números referentes aos ciberataques em Israel quase duplicaram. Houve perdas muitos assinaláveis e isto tendo por base apenas as que foram reportadas (cerca de 30% do valor total) porque muitas instituições nem reportam os seus danos e perdas num ciberataque.

Atualmente, na sequência destas ameaças, **as estruturas das organizações podem passar 14 a 16 dias inoperáveis. A média é que um ataque demora 9 dias a ser implementado e depois são mais 14 dias até chegar uma primeira reação da vítima**.

Há menos de um ano os ciberataques em Israel exigiam, quase sempre, a libertação de pessoas ou eram ataques contra o regime aos quais se seguiam as exigências de libertação. Quem o fazia não estava interessado em dinheiro, mas sim no grande impacto sociológico e psicológico que este tipo de ataques provocava. Hoje os israelitas estão a ser atacados pelo roubo de *passwords*; tudo tem mais a ver com o fator humano e com a destruição dos dados.

A nossa vulnerabilidade está à vista e, cada um de nós, é, de certa forma, culpado do que se vive, uma vez que estamos cada vez mais digitais e mais dependentes da opinião pública do que os atacantes.

Os terroristas modernos em vez de saberem construir submarinos ou aeronaves, têm profundos conhecimentos de como se comporta o mundo digital e atuam em conjunto, formando super-grupos de *hackers* que temos de conseguir combater. **“São os valores do mundo anti-democrático que estão aqui em causa e esses grupos entendem muito bem as assimetrias do mundo atual”**, refere Yigal Unna. Hoje estamos a ser atacados pelo roubo de *passwords*; tudo tem mais a ver com o fator humano.

Phishing é um dos ataques mais populares e ocorre devido a *passwords* fracas e à intervenção humana. Imaginemos um ataque à Microsoft… com os logos quase iguais, com os nomes escritos com um grafismo muito semelhante ao original… está comprovado que mais de 40% das pessoas clicam no link. **O elo mais fraco é o fator humano.**

O Israel National Cyber Directorate Former Chief lembra que são muitos os exemplos que, em jeito de paródia até circulam pela Internet, com *passwords* escritas e impressas em locais tão visíveis que chegam a aparecer em imagens de fotografia e vídeo.

Um dos ataques civis russos mais graves de sempre, perpetrado à empresa Solar Winds, aconteceu por causa do **fator humano precisamente pela certeza de que o utilizador vai fazer alguma asneira.**

Noutros contextos de guerra, uma arma simples causaria um dano reduzido em duas ou três pessoas. Mas a natureza das armas de ciberataques é que **mesmo essa arma simples** (um conjunto de letras e números num computador ligado à Internet) **pode resultar num grande ataque, envolvendo engenheiros e armas massivas capazes de estudar as capacidades dos países**. A Era Ciber é a mais complicada de todas de gerir, porque se baseia em conhecimento que se obtém em qualquer lado. Estas são as novas regras que podem ter dimensões dez vezes superiores à bomba de Hiroxima e o que se está a verificar é que **os decisores não compreendem completamente o que está a acontecer.**

"Em 2016 percebemos em Israel que temos que proteger tudo e foi decidido levar-se por diante essa decisão em três camadas: infraestruturas críticas, infraestruturas essenciais (hospitais e bancos) e proteção à população. Podemos ligar o 112 em Israel e ter uma resposta humana sempre do outro lado, o que ajuda em qualquer *ciber related issue*", refere Yigal Unna.

O especialista deixou-nos, no final da sua apresentação, três grandes lições:

1. **Não esperar pelo regulador**. As pessoas são iguais em todo o lado e vamos saber lidar bem com as situações em antecipação ao que o regulador vai decidir;

2. **Estabelecer parcerias. Não se vence sozinho o combate contra a cibersegurança** e é muito perigoso ter, na infraestrutura, alguém com um grande ego e que se ache o líder deste combate;
3. **Rapidez de reação aliada a um bom backup**. O que aconteceu ontem e resultou, hoje já não funciona porque as combinações de pessoas e tecnologias são infinitas. Um *backup* "hot", com toda a informação junta e ligada entre si é mais vulnerável; um *backup* "cold", com tudo separado por vários servidores e disconectado, é mais robusto. Depois de se ter um bom *backup* é preciso treinar muito e simular tentativas de recuperação. "Não se pode esperar que o acidente aconteça para se experimentar se o *backup* resulta", conclui.

Na mesa-redonda moderada por **Nuno Guerra Santos**, Vogal da Direção da APDSI, o debate centrou-se na visão de cada um dos intervenientes em cibersegurança e como as organizações podem caminhar rumo a um maior estágio de maturidade no combate ao cibercrime.

Frederico Macias, lidera a prática da cibersegurança na Deloitte, e apercebeu-se que há alguns países que são um alvo prioritário para os ciberataques o que levanta a curiosidade sobre em que ponto Portugal estará para os atacantes e que caminho o país pode seguir para se tornar mais robusto no combate.

O primeiro ponto, refere, **"é que não há risco zero. Um atacante encontra sempre um ponto de vulnerabilidade"**.

Para reduzir o risco e aumentar a resiliência há vários caminhos a seguir e um deles passa por ligar os vetores humanos aos tecnológicos, ou seja, aliar consciencialização, conhecimento, gestão de vulnerabilidades e uma *framework* de *zero trust*, que tem de ser um caminho importante e que voltou a estar em voga nas organizações.

A consciencialização passa por combater a obsoleta **cultura impositiva do *top down* em que as pessoas tendem a não seguir o que lhes é imposto.** Empoderar os colaboradores é algo muito importante no processo porque são eles os melhores veículos da aplicação

de uma determinada cultura numa organização. Logo a seguir é preciso dar lugar à diversidade porque as pessoas têm diferentes consciências sobre cibersegurança. Da diversidade vêm os melhores caminhos a seguir, ajudados por uma boa comunicação que **“deve ser dirigida a quem nos ouve e vê e não apenas feita num único sentido, sem que alguém perceba”**.

O papel do responsável pela segurança (o CISO) deve ser o de criar alianças com os verdadeiros donos da segurança – o negócio. A confidencialidade é o ponto mais basilar da segurança da informação que tem um papel importante na margem de lucro da empresa.

O conhecimento é outra área importante a ter em conta, porque a formação é necessária para empoderar as pessoas e sensibilizá-las para a segurança. O retorno do investimento em formação é a prevenção dos ataques constantes, mas essa mudança não pode simplesmente fazer-se num plano anual porque os ataques e os vetores de ataque estão sempre a mudar. O risco que cada utilizador enfrenta é diferente e a informação tem de ser adequada a cada um deles. Se tal não acontecer, não há retorno positivo.

A gestão de vulnerabilidades tem vindo a ser feita com grande cuidado e dedicação na Deloitte, na medida em que, nos últimos anos, sempre que uma vulnerabilidade no sistema é exposta, o tempo de resposta tem vindo a reduzir, o que significa que esta gestão tem de ser muito mais rápida a fazer os *updates* nos sistemas. **A maturidade consegue-se aumentando o nível de criticidade da vulnerabilidade**. Muitas empresas não fazem esse caminho de proteção, mas na verdade é de simples execução. As ameaças existem dentro e fora da rede, o que obriga a mais políticas de segurança e autenticações fortes porque o utilizador também não tem sempre a mesma relação com a empresa e o seu computador pode ter sido comprometido e ele nem saber.

O *zero trust* é uma tendência para se desenvolver no caminho. Os setores são muito diferentes (uns mais regulados que outros) e a regulamentação acelera muitos processos. Exemplo disso é **o setor da banca que responde imediatamente a normas internacionais, mas o setor público e o privado têm níveis de maturidade diferentes.**

O futuro passa por motivar mais as equipas e dar mais capacidades de atuação às pessoas e *frameworks* para abrirem caminho à transformação digital das organizações.

José Galamba de Oliveira, Presidente do Conselho de Direção da Associação Portuguesa de Seguradores, descreve que o objetivo primordial da Associação é proteger as companhias de seguros que também vendem proteção, logo estão preocupadas com a muita informação em bases de dados, que é muito rica, está acumulada há muitos anos e é informação muito sensível, principalmente no caso da saúde. Nos últimos anos tem havido uma tendência para deixar de se olhar para este problema como algo de IT, dando lugar a uma consciência coletiva de que este é um tema de pessoas e monitorizado em toda a organização. A prioridade é proteger a organização.

80% dos casos de questões relacionadas com cibersegurança são originados por má prática humana. **"No dia a dia, em tudo o que fazemos, temos que ter uma atenção muito grande sobre com quem estamos a interagir do outro lado"**, adverte José Galamba. Nesta relação, os testes são bons para se verificar a quantidade de pessoas que abrem um anexo ou um link. **"A maioria cai na armadilha embora haja duas organizações que estão a fazer testes trimestralmente, e já notaram uma redução de 15% no número de cliques potencialmente perigosos que dão"**, refere o presidente.

Antes de se fazer um seguro em cibersegurança, é preciso desmistificar a ideia de que com um seguro ciber os responsáveis pelas empresas estão protegidos.

A indústria dos seguros em cibersegurança está muito desenvolvida nos Estados Unidos (80% dos seguros em cibersegurança são lá; 10% estão no UK e o resto do mundo detém os outros 10%). Nota-se uma dificuldade na partilha de informação para se fazer uma análise correta. A América é um centro de inovação tecnológica muito grande, por isso, os profissionais partilham essa informação com o setor segurador e na Europa o caminho está por fazer.

Em Portugal, já existe alguma oferta para as PMEs feita com serviços de um conjunto de parceiros. O que se pretende é que ao longo do contrato de seguro se mantenha a preocupação de que há sempre risco (aumentando a sensibilização das pessoas), mas é

feita uma avaliação contínua do grau de maturidade dos sistemas, o que também ajuda a traçar um caminho. O setor tem um papel de polícia em relação a um plano de ação e no futuro será de esperar um setor segurador mais interventivo. Muitos destes riscos são globais e internacionais. Na Europa esse conhecimento do que já é feito internacionalmente tem de chegar ao setor segurador.

José Galvão, Diretor de Sistemas de Informação do Grupo Impresa, começou por dizer que nenhum ataque em Portugal é comparável àquele de que foram alvo.

A SIC foi uma das primeiras plataformas portuguesas paga com transmissões de *streaming* por IP. Houve uma destruição massiva de infraestrutura, mas sem perda de arquivo. **“Se o jornal saiu nas datas em que estava previsto, foi porque tínhamos um plano de contingência e agora a Impresa tem um orçamento mais generoso para a área da cibersegurança”**, com equipas dedicadas e planos, **“mas estamos conscientes de que um ataque pode acontecer a qualquer um e a qualquer empresa”**.

Durante o período mais crítico do ataque, as grandes preocupações da Impresa foram **“garantir a continuidade de negócio. Ninguém deixou de ver televisão apesar do ataque gravíssimo. Também tivemos a preocupação de controlar a temperatura dos *data-centers* porque senão perdíamos totalmente o controlo sobre as máquinas. Ao fim de uns dias os equipamentos iam falir. Em segundo, é importante haver sempre uma comunicação interna clara e com as autoridades: estejam preparados para pedir ajuda a quem sabe mais do que nós”**, descreve José Galvão.

Perante a ameaça de destruição massiva da infraestrutura não se consegue mudar tudo em simultâneo. Foi necessário implementar processos ágeis de gestão e **“tivemos que fazer *sprints*”** para alcançar determinados objetivos**.** Os planos de contingência foram priorizados, mas houve outras áreas que se revelaram mais penosas de recuperar.

“Temos que aproveitar um momento como este para mudarmos a forma de pensar. Os problemas atuais não resultam nem da falta de investimento nem de pessoas. É necessário, isso sim, promover uma mudança de mentalidade”, refere o responsável da Impresa. É aqui que entra o papel da educação em cibersegurança na criação de

ferramentas que permitam aumentar o nível de literacia para quem trabalha nas linhas editoriais.

Todos os planos de *backups*, de contingência e desastre são muito importantes, a par de garantir múltiplos fatores de acreditação. **Até vir a regulação tem de se dar passos no sentido de mudar políticas internas para as empresas serem mais ágeis** a adotar novas e saudáveis práticas.

Os media também podem ser relevantes nesta matéria, na medida em que houve imprensa estrangeira que descreveu o ataque à Impresa em moldes que não correspondiam à realidade. **O que deve ser divulgado? Apenas o que estiver previamente e completamente concertado com as autoridades**, porque há muita informação que não é produtiva que saia nos media. **“Para determinado tipo de ataques, saírem nas notícias só vem alimentar a promoção social dos atacantes, o que não favorece em nada”**, esclarece José Galvão.

A Impresa contacta com quatro milhões e 400 mil pessoas por ano. Mensalmente, no digital, são mais de quatro milhões de utilizadores únicos a quem o grupo alcança. No ambiente administrativo e de redação, são centenas de processos que entram na empresa diariamente.

Maria João Campos, Diretora do Centro de Gestão da Informação e Diretora do Serviço de Sistemas e Tecnologias da Informação e Comunicação do Centro Hospitalar Universitário de São João, reconhece que este, por ser um setor especialmente sensível, está totalmente aberto à inovação e à comunidade científica.

O São João é um hospital de referência para três milhões de utentes na região norte, com milhares de consultas e centenas de cirurgias diárias, onde a disponibilidade permanente dos sistemas é essencial. **De referir que os planos de catástrofe da OMS não contemplam as áreas ciber e hoje são uma realidade**. Para um hospital é fundamental fazer parte do plano de catástrofe nessa área, diz-nos Maria João Campos: **“estamos a mudar os planos de contingência e testados para algumas horas de indisponibilidade de sistemas. Um ataque destes, de forma massiva, pode implicar, pela ausência de informação clínica, a morte de pessoas”**.

A conformidade de um dispositivo técnico está de acordo com as vulnerabilidades do momento do seu lançamento e *compliance* com a prestação clínica, o que levanta desafios sobre como proteger estas áreas.

O Hospital tem trabalhado muito nas boas práticas para os sistemas, mas observando o que estava a acontecer com os milhares de dispositivos médicos foi necessário ter ferramentas ágeis automáticas que permitissem identificar vulnerabilidades, identificar e reduzir os riscos e convencer as áreas de negócio que **é preciso parar para atualizar a infraestrutura e aplicar os *patches de segurgança*.**

A sensibilização é essencial. Os clínicos trabalham com centenas de aplicações e não se consegue fazer a dupla autenticação, portanto, é muito complicado numa consulta com tempo limitado, colocar mais sistemas em que o profissional de saúde tem de se autenticar e ser-lhe exigido que o faça de uma forma mais ágil.

A comunidade médica ainda não está sensibilizada para as questões de cibersegurança, embora o tema já esteja nas agendas do Ministério da Saúde, mas ainda não faz parte da cultura do próprio Ministério.

A Diretora do Centro de Gestão da Informação do Centro Hospitalar Universitário de São João acredita que, para colocar o tema na agenda da Saúde, é preciso ver oportunidade nos investimentos que virão com os PRRs. A Saúde terá, pelo menos, direito a trezentos milhões de euros no âmbito deste fundo e será uma boa altura para se investir de forma estruturada.

Para Maria João Campos, o Ministério deveria trabalhar com fornecedores, parceiros e indústria porque **"as soluções trabalham-se em conjunto para melhorar a nossa ciberresiliência"**.

No encerramento da sessão, **o Contra-Almirante António Gameiro Marques, Diretor-Geral do Gabinete Nacional de Segurança, partilhou que aprendeu nesta sessão que "desde que temos consciência de nós próprios que somos seres que vivem no espaço físico e virtual. Porque quando começamos a ter consciência de nós próprios, criamos um modelo mental que depende da forma como fomos educados, vivemos e passamos**

toda a vida a tentar sincronizar esse mundo físico com o mundo virtual". Simplificando, cada um de nós depende desse sincronismo entre os mundos virtuais de uns e outros. A nossa memória está sempre a tentar sincronizar o mundo físico com o nosso virtual e o dos outros.

Neste desafio permanente, em que as pessoas são o denominador comum, tudo se centra nelas, portanto, temos que promover a combinação de saberes de todas as áreas de conhecimento, porque só assim conseguimos percebê-las: modular e adaptar a comunicação ao público-alvo.

Para o Contra-Almirante, a comunicação e formação sobre cibersegurança deveria ser feita numa lógica semelhante à do funcionamento dos *influencers* para os mais jovens, isto é, deveria ser dada por gente que trabalha para a faixa em que nos inserimos e outro grupo deveria falar para as pessoas com mais idade, sempre com o foco nas suas prioridades, combinando saberes e gerações porque "ninguém pode ficar de fora".

90% das vezes os problemas são causados por fator humano, de qualquer nível; qualquer um de nós pode ser o *leak in the chain*.

Por oposição a Daniel Traça, *Dean* da NOVA SBE - School of Business and Economics, **António Gameiro Marques defende que as pessoas conseguem ser bastante criativas em ambiente de terror e de tensão**, como a guerra, **"que fomenta a criatividade do ser humano"**. Também defende que **a infraestrutura mais crítica que temos que proteger é a democracia, até porque os países democráticos são uma minoria atualmente (37,8%)** e esse modo de vida tem de ser protegido.

É preciso proteger infraestruturas críticas, serviços essenciais e a cadeia de abastecimento, recorrendo, sempre que possível, a parcerias: **"a cooperação com compromisso, entre pessoas e gerações diferentes, gera confiança. Queremos sobreviver e voltar mais fortes de um ataque".**

Ao final da manhã, **foi feita uma visita ao Ciber Gym Digital Experience Lab. Tiago Godinho, o responsável por esse espaço virado para o futuro num mundo cada vez mais digital, também defende que a literacia digital é muito importante** para os executivos (os de hoje e os de amanhã).

As tecnologias oferecem boas oportunidades para a gestão, mas também existe a componente dos riscos que inspirou a criação deste Ciber Gym Digital Experience Lab no qual foi feita uma parceria com a INCM - Imprensa Nacional Casa da Moeda - para uma oferta de formação voltada para a ciberliteracia.

A ideia do Ciber Gym era fazer parcerias e partilhar conhecimentos com infraestruturas reais e partilha com a comunidade. Tudo é real neste campo de treino.

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 e Privacidade, a Ética no Digital, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, as Tecnologias de Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação, as Competências digitais e o Ambiente e Energia.

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

Apoio Institucional

NOVA SCHOOL OF BUSINESS & ECONOMICS

Patrocinadores Globais da APDSI

Platina

accenture aws Google

Ouro

devoteam Meta