IInova

Nº 2 abril 2022 | ISSN 2795-4633

INSTITUTO DE INFORMÁTICA

JUNTOS
Pela Ucrânia

PORTUGAL FOR UKRAINE

Instituto de Informática tem em curso ações no âmbito do acolhimento de refugiados da Ucrânia

ENTREVISTA COM O COORDENADOR DO CNCS

Em entrevista à IInova, Lino Santos fala do papel do Centro Nacional de Cibersegurança

IMPACTO AMBIENTAL DAS CRIPTOMOEDAS

Como a produção das criptomoedas pode traduzir-se numa ameaça para o meio ambiente

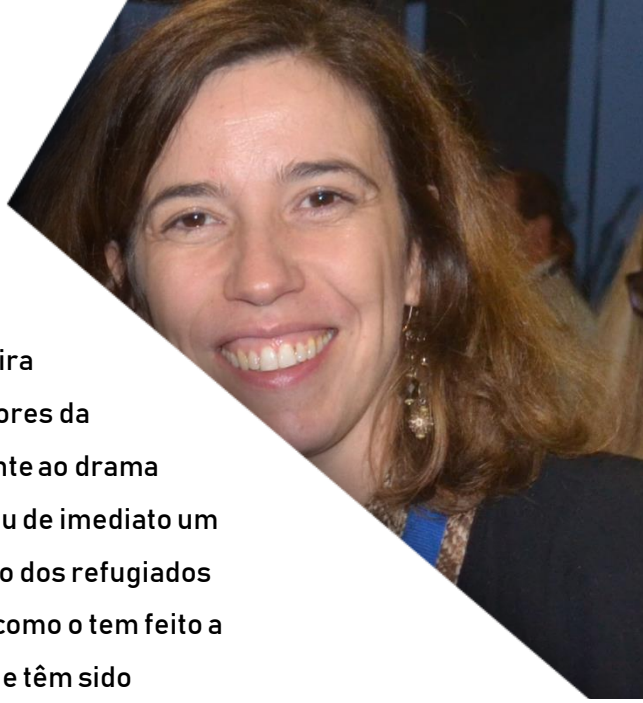
Periodicidade trimestral | Distribuição gratuita

ÍNDICE

FICHA TÉCNICA

Diretora: Paula Salgado
Editora: Joana Vallera
Redação: Helena Silveirinha, Mara Hentschke, Rita Teixeira
Design: Sofia Pinto Geada
Conselho Editorial: Anaísa Sousa, Ana Ribeiro Cruz, André Anjos, Célia Vasconcelos, Helena Silveirinha, Luísa Cordeiro, Nuno Costa, Patrícia Jesus, Pedro Diogo
Propriedade: Instituto de Informática, I.P.
Morada: Av. Prof. Dr. Cavaco Silva, 17—Tagus Park—2740-120 Porto Salvo
ISSN 2795-4633

Editorial



O número 2 da revista INova tem como capa a bandeira da Ucrânia, símbolo máximo de uma nação. Tem as cores da Ucrânia como capa pois ninguém pode ficar indiferente ao drama que se passa naquele país. O Estado português lançou de imediato um conjunto de medidas que visam o acolhimento e apoio dos refugiados que procuram abrigo e segurança no nosso país, tal como o tem feito a sociedade civil através de uma série de iniciativas que têm sido levadas a cabo. No que se refere ao Instituto de Informática também temos estado na linha da frente, com um conjunto de ações que temos aqui oportunidade de partilhar.

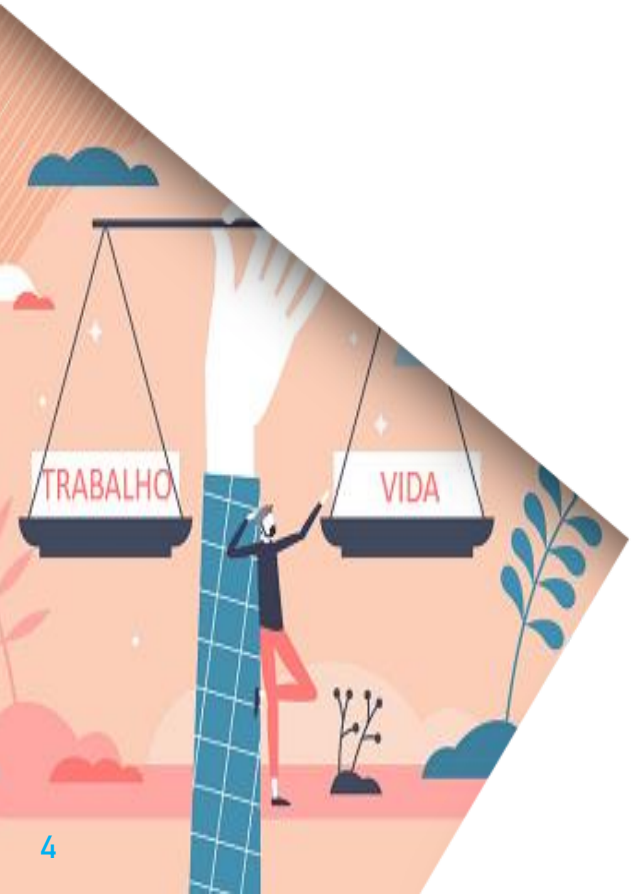
São tempos estranhos os que vivemos, e que certamente já não contaríamos assistir. Às novas formas de guerra, que tivemos oportunidade de abordar na 1.ª edição ao falar das ameaças híbridas, junta-se a guerra convencional, com artilharia pesada. À conversa com o coordenador do Centro Nacional de Cibersegurança, Lino Santos, percebemos como se combate nestas várias frentes. Na entrevista dada são também deixadas pistas importantes de como os organismos devem agir no âmbito da cibersegurança, área cada vez mais central e crítica na atividade de todos.

Nesta edição falamos ainda do que se faz cá dentro, mas também do que é feito noutros organismos, partilhando as boas práticas que se vão espalhando pela Administração Pública. Trazemos um olhar diferente sobre a tecnologia associada à produção das criptomoedas e partilhamos o novo jogo da moda, que nos apresenta um desafio diário que consiste em descobrir a palavra do dia, que tem sempre 5 letras. O nosso desejo é que a palavra a descobrir seja любов.

PAULA SALGADO | Presidente do CD do Instituto de Informática, I.P

Instituto de Informática avança com implementação do Sistema de Gestão da Conciliação

O Instituto de Informática aderiu em 2019 ao IGEN – Fórum Organizações para a Igualdade, e decorrente do **Programa 3 em Linha** procedeu à assinatura do **Pacto para a Conciliação**, tendo também apresentado uma candidatura com vista à implementação de um **Sistema de Gestão da Conciliação entre a vida profissional, pessoal e familiar** ao abrigo da NP 4552:2016. Este projeto teve o seu início no último trimestre do ano de 2021, estando já concluída a fase de diagnóstico.



A implementação de um **Sistema de Gestão da Conciliação (SGC)** dá a possibilidade de identificar e considerar as necessidades e expectativas das principais partes interessadas, definir e implementar as políticas, os procedimentos, os programas e as práticas adequadas ao contexto da organização e ao perfil dos seus trabalhadores e trabalhadoras.

Fazendo a conciliação parte dos 17 Objetivos de Desenvolvimento Sustentáveis para 2030, o Sistema de Gestão da Conciliação entre a Vida Profissional, Familiar e Pessoal, será mais uma ferramenta para alavancar a sustentabilidade organizacional e a responsabilidade social, à semelhança do que está também a ser feito por outras entidades do MTSSS, promovendo o bem- estar de todos os que trabalham no Instituto de Informática e a satisfação das necessidades e expectativas dos parceiros, cidadãos e empresas, através da disponibilização de melhores serviços.

sigä Analytics

O Sistema de Informação para a Gestão do Atendimento – sigä, tem um novo módulo de Analytics, com dashboards dinâmicos, de fácil consulta e visualização.
A apresentação da informação agregada permite efetuar de uma forma simples, análises comparativas, como a do nível de desempenho e da procura de serviços, num importante contributo para a gestão dos serviços de atendimento.

Presente em 1.441 serviços de atendimento, distribuídos por 13 entidades de Portugal Continental e Regiões Autónomas, o sigä torna-se cada vez mais um importante aliado na gestão do atendimento dentro da Administração Pública.

PORTUGAL FOR UKRAINE

A recente invasão da Ucrânia por parte da Rússia levou a que milhares de ucranianos e outros residentes, saíssem do país, em fuga de um cenário de guerra. Tal como o resto da Europa, Portugal solidarizou-se com este drama, disponibilizando-se para ajudar e acolher os refugiados.

Foram várias as iniciativas a surgir por parte da sociedade civil, mas também do Estado Português que rapidamente lançou um conjunto de medidas de apoio e de integração e acolhimento das pessoas deslocadas, sistematizadas no portal Portugal For Ukraine.

São já muitas as ações implementadas no terreno, com o Instituto de Informática também a ser chamado a dar resposta a um conjunto de necessidades e desafios para garantir o apoio às famílias refugiadas de forma ágil.

Foi criado, no Portal da Segurança Social, um microsite para uso exclusivo de informação no âmbito da operação de refugiados;
Foram feitas adaptações no subsistema de Identificação para permitir registar a identificação de refugiados;

Foi implementado um processo de registo de identificação em IDQ, através da solução de RPA (Robotic Process Automation), que permite a atribuição de NISS, sem intervenção humana, para comunicação ao SEF para inclusão das Declarações de Proteção Temporária;

Monitorização da Operação – Refugiados da Ucrânia, através da implementação de *dashboard* em *power* BI com atualização da informação relevante para monitorização das atividades do MTSSS;

Envio de Notificações Massivas de E-mail em português, inglês e ucraniano, com a informação dos NISS criados;

Realização de trabalhos com vista à implementação de serviços de interoperabilidade entre o SEF e a Segurança Social, com vista à atribuição automática de NISS e à receção da autorização de permanência em Portugal.

A vontade de ajudar é grande e transversal, multiplicando-se as iniciativas, individuais ou coletivas, particulares ou institucionais, numa tentativa de levar bens essenciais a quem neste momento precisa e de acolher aqueles que procuram um porto seguro.

Catarina Reis

49 anos

Colaboradora do Instituto de Informática

Voluntária na campanha SOS Ucrânia

O que a levou a ajudar?

Como todos nós fiquei chocada com o que estava a acontecer, sentindo-me impotente e assustada com o facto de serem pessoas como nós, com vidas organizadas e estruturadas como a minha e que de repente perderam tudo. Fez-me pensar, e se fosse comigo?

Tinha de ajudar. Comecei a pesquisar como podia fazê-lo e encontrei a campanha SOS Ucrânia da Câmara Municipal de Cascais. Inscrevi-me e fui chamada. Primeiro para integrar a equipa que faz a triagem dos bens doados e organiza os mesmos para serem levados até às fronteiras com a Ucrânia, e depois, devido à minha formação base como psicóloga, para ajudar na receção aos refugiados que vinham através de um voo organizado pela Câmara.

Como foi receber os refugiados?

Era um grupo só de mulheres, crianças e adolescentes. Eram poucos os idosos. Chegaram já tarde, vinham muito cansados e acabou por não haver muita interação. Mas senti que estava a ajudar e isso foi muito gratificante. Sinto o mesmo quando estou a separar os bens e imagino que os mesmos se destinam a pessoas que neste momento estão a precisar deles.

Quando viu as pessoas saírem do autocarro, em que pensou?

Pensei que podia ser eu. No dia seguinte acordei a pensar no que estariam elas a pensar e a sentir. Agora o que me tem passado pela mente é que trazer estas pessoas foi a parte mais fácil. Mas o que vai ser do seu futuro?

ENTREVISTA

Coordenador do CNCS

Centro Nacional de Cibersegurança

Fazendo jus à doutrina pregada, é através da passagem por vários controlos de acesso que chegamos ao gabinete do coordenador do Centro Nacional de Cibersegurança (CNCS). À frente do centro que tem como missão contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional, Lino Santos fala-nos dos principais riscos que enfrentamos, mas também daquilo que cidadãos e empresas, mas principalmente a Administração Pública pode fazer para mitigar os mesmos.

Os recentes ataques cibernautas ocorridos em Portugal (grupo Impresa, Vodafone, Laboratórios Germano de Sousa), que apanharam um pouco de surpresa a sociedade, fizeram soar os alarmes sobre o perigo e impacto que este tipo de ataque pode ter. Qual é o verdadeiro risco que corremos?

Pode ter apanhado de surpresa a sociedade porque, e pensando em particular nos incidentes da Impresa e Vodafone, visaram duas entidades em que o impacto foi bastante percebido no dia a dia das pessoas. No entanto, o ritmo e a cadeia como os incidentes têm ocorrido em Portugal tem mantido uma tendência de crescimento sustentado nos últimos anos.

Temos 80% de crescimento de incidentes em 2020 relativamente a 2019, tivemos uma taxa menor de crescimento, cerca de 30%, em 2021 relativamente a 2020, e no início deste ano, em período homólogo do ano passado, temos uma duplicação do número de incidentes. Portanto, esse crescimento tem-se apresentado de forma sustentável. Agora temos muitos incidentes que não têm este perfil mediático que estes dois incidentes tiveram e isso foi de facto o que apanhou de surpresa o cidadão comum.

Face a esse crescimento da criminalidade, que foi até contraciclo face à criminalidade convencional, que essa sim desceu, crê que o cidadão tem essa perceção de que está a aumentar o risco que corre e as vulnerabilidades a que está sujeito?

Julgo que ainda há muito trabalho a fazer no que diz respeito à sensibilização dos cidadãos. Obviamente que estes ataques em particular, que referimos, ajudam a essa consciencialização, mas queria também frisar que esta tipologia de ataques não é a mais comum dentro do total de ataques que tratamos. Só para ter uma ideia, cerca de 40% dos ataques que são tratados pelo Centro Nacional de Cibersegurança são ataques relacionados com o que chamamos, de uma forma genérica, de engenharia social, ou seja, esquemas de fraude, de furto de identidade, onde normalmente o vetor de exploração é o fator humano. É o clicar no link que não devia. Normalmente há uma narrativa por trás, normalmente a levar o utilizador a querer clicar, ou querer abrir um anexo ou uma mensagem de correio eletrónico. Agora se há uma consciência por parte da população relativamente a este assunto, eu diria que sim, embora ainda haja muito trabalho a fazer nas componentes de alteração de comportamento, de alteração de atitudes por parte do cidadão. Isto note-se, tem depois também implicações na cibersegurança das organizações.

> "O DL 65/2021 prevê uma metodologia (...) que passa por inicialmente realizar uma análise de risco"

O cidadão comum com determinadas atitudes e comportamentos é um risco para a organização quando esses comportamentos não são os ideais. Aí há um grande trabalho da nossa parte, através dos nossos cursos online que designámos de competências básicas em cibersegurança. Estamos a falar das componentes de ciberhigiene, relacionadas com as questões das passwords seguras, de fazer os backups, de como é que se utilizam os dispositivos amovíveis, coisas muito básicas que devem ser

tornadas naturais. Mas também temos cursos focados na segurança de compras online, na segurança de utilização de redes sociais e também um curso dedicado ao tema da desinformação, para de alguma forma ajudar os utilizadores a distinguir o que é informação correta de *fake news*.

Fazendo a ponte para as organizações e o Decreto-Lei n.º 65/2021, que prevê a obrigatoriedades dos organismos da Administração Pública apresentarem ao CNCS um relatório anual no âmbito da segurança de informação, que preocupações devem ter e como acautelar o seu cumprimento?

O DL 65/2021 prevê uma metodologia. É um conjunto de obrigações, mas de alguma forma tem embebida uma metodologia, que passa por inicialmente realizar uma análise de risco, ou seja, nem todas as organizações são iguais, nem todas as organizações estão sujeitas aos mesmos agentes de ameaça, nem todas as organizações tratam o mesmo valor de informação, nem todas as organizações têm serviços críticos ou essenciais. Portanto, começar o trabalho, e depois fazê-lo de uma forma sistemática ao longo dos anos, mas começar o trabalho por fazer uma análise de risco, muito focada naquilo que são as joias da organização do ponto de vista informacional, naquilo que são os serviços essenciais, é extremamente importante para determinar o que é necessário fazer do ponto de vista do plano. Realizada essa análise de risco, chegamos a um resultado que é uma lista ordenada dos riscos e uma valorização de cada um dos riscos que a organização corre. Depois o que dizemos no DL 65 é procurar no quadro nacional de referência e cibersegurança (temos um referencial que criámos em 2018 para a cibersegurança nacional) quais são as medidas que mitigam cada um daqueles riscos, e isso compõe o plano. É lógico que isto implica algum investimento por parte das organizações, é lógico que implica uma alteração da cultura de segurança dentro das organizações, mas é precisamente isso que pretendemos atingir no final. É esta gestão cíclica da realização de análises de risco, com implementação de medidas que estão no quadro nacional de referência, que mitigam os riscos identificados. Não há uma receita que sirva todas as organizações, o que existe sim, é uma metodologia que leva as organizações a reduzirem o risco a um nível aceitável.

Até que ponto é que o PRR pode alavancar a temática da cibersegurança dentro das organizações? A verba de 47M€ para reforço do quadro geral de Cibersegurança na Administração Pública é suficiente para o que é necessário fazer?

Temos aqui duas dimensões. A verba específica que refere prevê a criação de um conjunto de instrumentos dentro do Centro Nacional de Cibersegurança para apoio, quer à Administração

> "estamos desde o início do conflito na Ucrânia em modo de *full cooperation*"

Pública quer à economia do ponto de vista da capacitação de pessoas, portanto criação de competências na área da cibersegurança e capacitação de organizações, ou seja, o crescimento na maturidade de organizações públicas e privadas. Isto significa que, ainda este ano, vamos arrancar com uma academia de cibersegurança que tem por objetivo formar um conjunto de 10.000 especialistas em cibersegurança até ao final do período de apoio do PRR, previsto para final de 2025. Isto vai permitir que as organizações tenham uma oferta formativa adequada à implementação das referidas medidas do quadro nacional de referência e cibersegurança.

Já temos uma oferta formativa de cerca de 42 cursos, vamos agora celebrar os acordos de parceria com as entidades formadoras para em setembro, se tudo correr bem, arrancar com as primeiras ações de formação. Mais uma vez, a ideia não é que as organizações tirem 42 cursos em cibersegurança, a ideia é com a análise de risco que realizam, verifiquem quais são as medidas que têm de aplicar e para cada uma dessas medidas têm de certeza pelo menos um curso que dá as competências para a sua boa implementação.

Para a criação de competências nas organizações, vamos criar durante este ano uma rede de centros de competências, que no fundo são braços armados do CNCS em cada uma das regiões do país, incluindo ilhas. Vamos ter estes centros de competências, muito provavelmente com parcerias entre associações empresariais e industriais e a academia, para chegar o mais próximo possível da administração local, o mais próximo possível do tecido empresarial local, com os referenciais e com os instrumentos que criámos aqui centralmente no Centro Nacional de Cibersegurança.

Temos assim esta lógica do PRR como criação de instrumentos para ajudar a criação de competências e a criação de maturidade em cibersegurança das organizações. Mas depois temos os PRR individuais de cada um dos organismos da administração pública e aqui só posso deixar um conselho, de que desde o início considerem a cibersegurança como um elemento, ou como uma alavanca nos processos de transição ou de digitalização que tenham previstos dentro do PRR, ou seja, uma abordagem *cibersecurity by design*, uma abordagem de avaliação de risco, pois cada vez que enveredamos por um processo de digitalização estamos a aumentar a nossa superfície e portanto deve ser coadjuvado com um conjunto de medidas que reduzam os novos riscos introduzidos por esses processos de digitalização. Essa é uma responsabilidade de cada um dos organismos da administração pública que gerem esses mesmos investimentos.

Não temos só 47M€ para aplicar em cibersegurança. Temos 47M€ para um conjunto de instrumentos que vão ser criados centralmente pelo Centro para estas organizações, mas depois temos os projetos individuais que devem obviamente ter à cabeça o *cibersecurity by design* na sua

Saindo da esfera nacional, estamos a assistir, no atual conflito que ocorre na Ucrânia, a mistura da guerra convencional e da guerra de propaganda e no ciberespaço, com tentativas de controlo e de bloqueio à própria internet. Como é que se combate nestas várias frentes?

O Estado tem um conjunto de instrumentos para lidar com estes conflitos. Não existe um instrumento único, ou seja, este tipo de conflitos requer uma intervenção ao nível da proteção, com a aplicação de medidas extraordinárias de proteção, com o reforço da resiliência das organizações, aqui a pensar em particular nas infraestruturas críticas e nos operadores de serviços essenciais mas também na Administração Pública, nos serviços essenciais da Administração Pública, numa componente de resposta a incidentes muito focada na recuperação e na continuidade da atividade, ou seja, uma lógica quase de bombeiro da internet. Se ocorre uma situação e é preciso repor a normalidade, essa é uma função do CNCS, através da sua equipa de resposta a incidentes de cibersegurança, mas depois tem um domínio de atuação de investigação criminal e prossecução judicial, tem um domínio de atuação na área da diplomacia da cibersegurança, por exemplo, observámos isso com a aplicação de sanções e no caso de perigarmos a soberania nacional e interesses nacionais, poder usar o ciberespaço como domínio de operações, sendo aqui um monopólio das Forças Armadas. Numa situação complexa como esta temos de estar preparados para usar estes diferentes instrumentos que estão ao serviço do Estado para este tipo de conflitos e é isso que de alguma forma é feito todos os dias com as articulações que mantemos.

Isto a nível nacional. E o CNCS tem relação com outras entidades europeias congéneres?

O CNCS atua naquele primeiro eixo de atuação que referi, da resiliência e da resposta a incidentes. Nesse contexto, a nossa equipa de resposta a incidentes de

cibersegurança faz parte de uma rede europeia de equipas de resposta a incidentes de cibersegurança e aí estamos desde o início do conflito na Ucrânia em modo de *full cooperation*, com partilha de informação sobre todos os incidentes que possam estar relacionados com esta situação geopolítica, partilha de indicadores técnicos, ou seja, o que procuramos é a partilha de informação que seja acionável na defesa individual, depois nas nossas organizações.

A informação que bebemos deste fórum é traduzida em recomendações de proteção para os nossos públicos de interesse, que são os operadores essenciais, os operadores de infraestruturas críticas e a Administração Pública. Isto numa camada técnica.

Numa camada operacional também funcionamos em rede com os restantes Estados-Membros no que se chama a rede Ciclone, que é uma rede para gestão de crises a nível europeu nesta área da cibersegurança e aí fazemos reportes sistemáticos sobre o estado da situação nacional no que diz respeito à cibersegurança relacionado com esta crise atual. Há assim estes dois fóruns, um mais técnico que procura informação acionável e um outro mais de criação de um quadro situacional europeu com o objetivo de informar a camada política sobre o que é que se está a passar neste ambiente ciber a nível europeu.

Para terminar, como vê o futuro da cibersegurança? Que preocupações estaremos a ter daqui a 5 anos?

Eu estou preocupado com a situação que temos hoje e, portanto, não posso deixar de recomendar a aplicação de um conjunto de medidas que tendo em conta aquilo que sabemos ser o *modus operandi* dos principais agentes de ameaça no terreno hoje em dia, podem ajudar as vossas organizações a sofrerem menos impactos de ciberataques. Talvez a mais importante seja a aplicação de um sistema de autenticação multifator. O mo*dus operandi* que temos vindo a observar desde o final do ano passado passa por adquirir credenciais comprometidas, ou previamente comprometidas, na *darkweb* para intrusão dentro das organizações. A partir do momento em que essa primeira intrusão é conseguida os objetivos destes agentes de ameaça podem ser o ganho financeiro, a destruição pura e dura ou a espionagem. Sendo o *modus operandi* a intrusão através da utilização de passwords previamente comprometidas, isto é mitigável se as organizações tiverem implementado no seu sistema mecanismos de multifator de autenticação.

Outras medidas que aconselhamos é uma atenção muito especial aos backups, ou seja, ter planos de recuperação bem testados, com backups que depois de produzidos são colocados offline, para que não sejam eles próprios sujeitos a um agente de ameaça, seja ele um esquema de extorsão online, mais conhecido por *ransomware*, ou outro.

Finalmente, estar preparado para reagir a um incidente. Isto tem um significado especial para a Administração Pública, porque tem obviamente dificuldades de contratação, em que contratar serviços não é feito de um dia para o outro. Aqui a ideia é estar preparado para reagir a um incidente que se venha a ter. Ter algum tipo de bolsa de horas, algum tipo de contrato já pré-definido com uma empresa de prestação de serviços de análise e resposta a incidentes é uma medida extremamente útil de preparação para o pior.

Orçamento participativo da Administração Pública

A Resolução do Conselho de Ministros n.º 130/2021 aprovou as normas que regem o Orçamento Participativo da Administração Pública (a par do Orçamento Participativo Portugal).

Este projeto visa posicionar as entidades da Administração Pública para dar o exemplo da adoção de processos participativos que envolvam os seus trabalhadores e trabalhadoras, colocando a sua valorização e boa gestão, no centro dos modelos de gestão pública, uma prática já levada a cabo no Instituto de Informática.

Para facilitar o processo de orçamento participativo, as entidades da administração pública podem recorrer à plataforma Participa.gov.pt disponibilizada pela AMA.

Saiba quais os passos necessários aqui.

A tecnologia ao serviço da inclusão dos idosos na Madeira

Cientes da importância de combater a solidão e isolamento dos idosos, o Instituto da Segurança Social da Madeira implementou nos cinco lares para idosos que tem sob a sua administração direta, o projeto siosLIFE.

Este projeto consiste em promover a inclusão social e digital dos idosos através da tecnologia, permitindo o reforço da componente lúdica, mas também o contacto com familiares.

Esta é uma das formas de colocar a tecnologia ao serviço das pessoas, não deixando ninguém para trás.

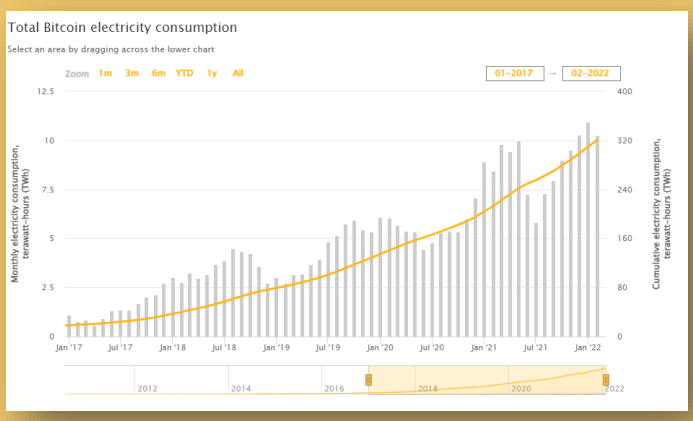
O IMPACTO AMBIENTAL DAS CRIPTOMOEDAS

As criptomoedas são moedas digitais, que não têm forma física, operando apenas no mundo virtual e sem a regulação de um banco central. A criação de criptomoedas está assente na tecnologia de blockchain, que se traduz em pedaços de códigos (os blocos), que ficam ligados entre si (a rede). É nesses blocos que ficam registadas informações, como os dados de transações das criptomoedas. A validação de transações é feita através de um processo de mineração. Para garantir que a informação é verdadeira, o minerador (computador) tem de resolver um algoritmo, conhecido como algoritmo de consenso, que confirma a veracidade. Como o minerador é recompensado pela operação que executa, quanto mais capacidade de mineração tiver, maior o rendimento que obtém. É aqui que surge o impacto ambiental.

Com a existência de cada vez mais mineradores, o algoritmo fica mais complexo e difícil de resolver, sendo necessário ter uma maior capacidade de processamento. Começaram a ser criados grandes armazéns, com milhares de computadores a operar 24 horas por dia, alimentados a eletricidade, muitas vezes produzida através de combustíveis fósseis ou até mesmo a carvão como nos conta um artigo do The Guardian, em que uma central a carvão foi reativada para a mineração de criptomoedas.

De acordo com um artigo do Jornal de Negócios, a produção de Bitcoin, uma das mais conhecidas criptomoedas, gasta quase o triplo da eletricidade consumida em Portugal. No já referido artigo do The Guardian, dá-se como exemplo que a energia utilizada para minerar a Bitcoin a cada 60 segundos seria suficiente para assegurar o consumo médio de uma família americana durante 17 anos.

Com as preocupações ambientais como pano de fundo, também esta área começa a procurar alternativas, com recurso a energias mais limpas ou renováveis. Para já o crescente consumo de energia é bem visível, como nos demonstram os dados disponibilizados pelo Centro de Finanças Alternativas (CCAF) da Universidade de Cambridge.



Evolução do consumo de energia pela produção de Bitcoin

Quebra-cabeças

Wordle é um jogo de palavras criado pelo programador Josh Wardle e daí o trocadilho com o seu nome. O objetivo é adivinhar uma palavra de cinco letras, em seis tentativas. Em cada tentativa, o jogador visualiza informação das letras que estão na posição certa e das que constam da palavra correta, ainda que não estejam bem posicionadas.

A lógica segue jogos clássicos como *Mastermind*, embora no caso do *Wordle* se informe exatamente quais letras que em cada palpite estão corretas. Há uma palavra de resposta específica para cada dia, que é a mesma para todos. O jogo tornou-se público em outubro de 2021 e, depois de ser criada a possibilidade de os jogadores compartilharem respostas e estatísticas, tornou-se viral, atingindo 2 milhões de utilizadores em janeiro deste ano. O jogo é gratuito e só pode ser jogado uma vez por dia.

O elevado número de jogadores atraiu a atenção do "*The New York Times*" que o adquiriu, por uma verba não divulgada, mas que se crê acima de um milhão de euros. As versões portuguesas não tardaram e já pode jogar a palavra-do-dia.

Pulseira eletrónica para ajudar triagem nos hospitais

A empresa criada por antigos alunos do Instituto Superior Técnico - JUNITEC, apresentou no âmbito do projeto CEiiA 2.0, uma pulseira que pretende monitorizar os sinais vitais dos pacientes que dão entrada na urgência hospitalar, permitindo através da transmissão dos dados por uma Web App que os profissionais de saúde possam gerir as prioridades do atendimento.

Esta ideia é uma das finalistas do *European Excellence Awards*, pela categoria "*Most Impactful Project*" e um bom exemplo da tecnologia ao serviço das pessoas.

Dicas Cibersegurança

Em colaboração com o CNCS, partilhamos algumas dicas para a adoção de comportamentos seguros no ciberespaço

| CASA SEGURA |

Proteja todos os seus dispositivos:

- Use passwords fortes e/ou autenticação de dois fatores (2FA);
- Altere a password definida e nome de rede: não inclua informação pessoal no nome de rede.

Verifique as aplicações:

- Descarregue aplicações apenas da lista oficial de aplicações (Google Play, Apple Store, etc.);
- Avalie as informações e autorizações solicitadas;
- Reavalie periodicamente a necessidade de manter todas as aplicações.

Verifique as definições de privacidade das contas nas redes sociais:

- Selecione, nas definições de privacidade, a informação que pretende incluir.

Ative as atualizações automáticas nos seus dispositivos e guarde cópias do que for importante offline ou na nuvem.

| SEGURANÇA DAS SUAS CONTAS |

Aposte na força da sua password.

- Quanto mais forte, mais difícil será piratear a sua conta. 15 caracteres combinados entre letras maiúsculas, minúsculas, números e símbolos, quando possível, irá garantir-lhe uma maior proteção.
- Utilize passwords únicas para todas as suas contas online.

Ative a autenticação multifatores (MFA)

- A autenticação MFA implica a apresentação de dois ou mais fatores para aceder a uma conta, por exemplo uma password e um código enviado para o telemóvel. Só na apresentação destes dois ou mais fatores será possível aceder à conta.

IInova

INSTITUTO
DE INFORMÁTICA
CONFIANÇA E INOVAÇÃO