# CIBERSEGURANÇA: O PAPEL DA ENGENHARIA INFORMÁTICA

JOSÉ MANUEL TRIBOLET
jose.tribolet@inesc.pt

PAULO FERREIRA
pjpf@tecnico.ulisboa.pt

MIGUEL CORREIA
miguel.p.correia@tecnico.ulisboa.pt

CARLOS RIBEIRO
carlos.ribeiro@tecnico.ulisboa.pt

PEDRO ADÃO
pedro.adao@tecnico.ulisboa.pt

NELSON ESCRAVANA
nelson.escravana@inov.pt

INSTITUTO SUPERIOR TÉCNICO,
UNIVERSIDADE DE LISBOA


## 1. INTRODUÇÃO

O ciberespaço[1] consiste no complexo ambiente virtual resultante do aparecimento da Internet, das pessoas e organizações que a utilizam e de todas as atividades, no diverso tipo de dispositivos e redes de comunicações que nela ocorrem. Apesar da sua intangibilidade, este mundo não é significativamente diferente do mundo físico, no qual a Engenharia desempenha um papel fundamental em assegurar o bom funcionamento da sociedade. O ciberespaço possui estradas (redes), edifícios (*software* e *hardware*) e as mesmas pessoas e organizações. Como tal, sofre de problemas semelhantes. A segurança do ciberespaço, ou cibersegurança, define-se como a segurança deste mundo virtual[2], o que inclui a confidencialidade, a integridade e a disponibilidade da informação e dos sistemas, entendendo-se sistemas na sua forma mais abrangente, incluindo as pessoas, o espaço físico e o ambiente (no caso dos sistemas ciberfísicos). Os domínios da segurança da informação, segurança de aplicações, segurança de redes de comunicação, segurança da Internet e a proteção das infraestruturas críticas de informação, encontram-se todos eles de alguma forma na esfera de atuação da Engenharia Informática e constituem os elementos basilares da cibersegurança (ver Figura 1).

A Contra-almirante Grace Hopper, por muitos considerada a "mãe" da Informática, afirmou: "Life was simple before World War II. After that, we had systems." Tal como nos seus congéneres do mundo físico, os cibersistemas (que incluem pessoas, organizações e tecnologia) são complexos e possuem propriedades emergentes, algumas das quais indesejáveis e imprevisíveis, propriedades essas que tipicamente resultam em vulnerabilidades sistémicas.

No entanto, as ameaças no ciberespaço possuem características únicas, tais como:

1 Termo cunhado por William Gibson, em 1982, na obra de ficção "Burning Chrome".
2 ISO/IEC 27032 – *Information technology – Security techniques – Guidelines for cybersecurity*.

a facilidade de automatismo, a capacidade de lançar ataques de regimes jurídicos distintos, a facilidade de difusão de informação sobre novas vulnerabilidades e métodos de ataque e a dificuldade de atribuição da autoria de um ataque. Estas propriedades aumentam a dificuldade de lidar com as ameaças no ciberespaço quando comparado com o mundo físico.

As principais ameaças da atualidade incluem o *malware* (vírus, vermes), o ataque a aplicações web, os ataques de negação de serviço, o *phishing* e o *ransomware* (que cifra dados e exige um resgate para a sua recuperação), afetando não apenas o tradicional domínio de IT, mas também os dispositivos móveis, os sistemas de controlo industrial (SCADA) e outros dispositivos permanentemente ligados (*Internet of Things*). Mais recentemente, a evolução do crime informático conduziu a investigação em cibersegurança para áreas menos clássicas da Engenharia Informática, como a designada "Engenharia Social", que utiliza meios informáticos para detetar e prevenir vulnerabilidades nos elementos humanos dos sistemas.

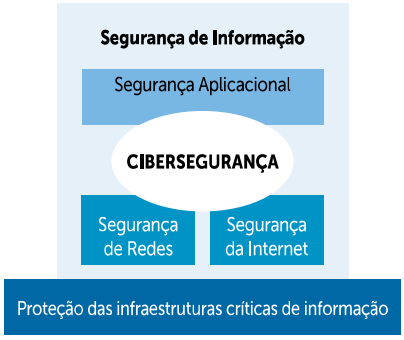


Figura 1 **Componentes fundamentais da cibersegurança**
(adaptado da norma ISO/IEC 27032)

A abordagem das organizações ao tema da cibersegurança resume-se frequentemente à segurança da periferia (*firewalls*) e do equipamento terminal (antivírus). Organizações com alguma dimensão recorrem à certificação ISO 27001 como a panaceia para o tema da cibersegurança. Apesar das normas ISO 27000 ajudarem a abordar o tema de forma estruturada, são manifestamente insuficientes em organizações que não possuem recursos humanos qualificados para conceber, adquirir e gerir os seus Sistemas de Informação e Comunicação (SIC) de forma adequada. Exemplo disso foi a "histeria" de algumas organizações a lidar com a recente ameaça do *ransomware* WannaCry e Petya que, por virtude de não dominarem a segurança dos seus sistemas, optaram em primeira instância por desligá-los da Internet. Apesar da acrescida complexidade deste domínio da Engenharia, da atual ubiquidade das TIC e do seu papel cada vez mais indispensável para a vida em sociedade, contrariamente ao que sucede com outras engenharias fundamentais para o seguro funcionamento da sociedade, a conceção de ciber-sistemas está praticamente isenta de qualquer regulação. Em acréscimo, esta atividade é exercida de forma anárquica, por indivíduos carecendo da devida formação académica e profissional, e isentos dos deveres deontológicos indispensáveis para assegurar a proteção da sociedade contra as naturais pressões do mercado sobre quem concebe, desenvolve, instala e mantém os SIC essenciais. Existe, no entanto, legislação nacional em vigor, como a Lei do Cibercrime que permite às organizações agirem judicialmente contra um alegado atacante nos raros casos em que a atribuição é possível. Foi recentemente aprovado um regulamento da União Europeia (UE) que entra em vigor em 2018 sobre a proteção de dados pessoais[3] que obrigará as organizações a medidas organizacionais e tecnológicas para salvaguardar a privacidade dos cidadãos contemplando elevadas coimas. Até 2018 deverá ainda ser transposta para a legislação nacional a diretiva para a segurança de sistemas e redes da UE[4], que obrigará os prestadores de serviços essenciais para a sociedade a um conjunto mínimo de práticas de cibersegurança. Na implementação destas regulamentações os engenheiros informáticos desempenham um papel nuclear, devendo garantir-se que possuem as competências fundamentais em cibersegurança.

## 2. O PAPEL DAS COMPETÊNCIAS FUNDAMENTAIS

A área da cibersegurança, tendo em conta o papel da Engenharia Informática, implica a consideração de duas vertentes fundamentais: a) a capacidade de compreensão das causas que estão na génese dos problemas detetados (i.e., *malware* em geral), e b) a capacidade de conceção, desenvolvimento, e aplicação das respetivas soluções. Para tal assume-se que existe, como conhecimento base, a) uma visão geral dos sistemas computacionais, desde conceitos de baixo nível (gestão de memória, processamento) até às camadas superiores, incluindo os sistemas operativos e os sistemas distribuídos, com ênfase nos aspetos mais diretamente relacionados com a cibersegurança, e b) uma visão geral dos sistemas móveis e na nuvem, incluindo conceitos como coerência, virtualização e bases de dados, focando os aspetos mais diretamente relacionados com a cibersegurança.

Assim, para que indivíduos ou organizações sejam capazes de endereçar as duas vertentes antes indicadas é absolutamente indispensável que disponham dos conhecimentos necessários especifica e diretamente relacionados com a cibersegurança. Estes conhecimentos podem ser agrupados nos domínios seguintes:

- **Segurança em computadores e das redes de comunicação**
  Este domínio engloba conceitos fundamentais subjacentes à cibersegurança em computadores, modelos de cibersegurança mais relevantes, modelo de ataques, mecanismos e algoritmos fundamentais de identificação, autenticação, criptografia e chaves, controle de acesso, monitores de referência, acesso a bases de dados e segurança do *software*, assim como conceitos fundamentais subjacentes à cibersegurança em sistemas distribuídos (i.e., em redes de computadores), mecanismos e algoritmos fundamentais usados nas comunicações em rede, código mal-intencionado, cifras, criptografia simétrica e assimétrica, assinaturas digitais, certificados e segurança nível transporte.
- **Segurança do *software* aplicacional e do *software* de suporte às redes de comunicação**
  Este domínio aborda as vulnerabilidades de segurança em *software* mais comuns, assim como as suas causas fundamentais e as soluções (mecanismos, algoritmos) para a sua prevenção e/ou deteção. Este domínio contempla ainda as vulnerabilidades de segurança mais comuns em redes de computadores e quais as respetivas soluções; nomeadamente, os principais erros

3 Regulamento 2016/679 do Parlamento Europeu e do Conselho.
4 Diretiva 2016/1148 do Parlamento Europeu e do Conselho.

na utilização e implementação de mecanismos de autenticação, na utilização de APIs criptográficas, assim como as principais vulnerabilidades dos protocolos da família IP, o que implica entender os conceitos essenciais para gestão de identidades, autenticação e autorização na Internet.

- **Segurança dos ambientes móveis (aplicações e *software* de suporte)**
  Este domínio contempla o conhecimento das vulnerabilidades de segurança que ocorrem em ambientes móveis, incluindo as suas causas fundamentais, assim como as soluções (mecanismos, algoritmos) para a sua prevenção e/ou deteção.
- **Segurança na Internet/Web, na nuvem e das bases de dados**
  Este domínio engloba as vulnerabilidades de segurança que ocorrem em sistemas na *web*, na nuvem e em bases de dados, assim como as suas causas fundamentais; contempla também as respetivas soluções (mecanismos, algoritmos) para a sua prevenção e/ou deteção, incluindo a deteção de intrusões e a segurança da cadeia de fornecimento.
- **Testes de segurança ao *software* e o seu desenvolvimento seguro**
  Este domínio aborda os riscos de segurança associados aos SIC, os respetivos conceitos fundamentais subjacentes ao teste de *software* seguro, o seu desenvolvimento e aplicação no contexto de testes de segurança abordando as técnicas e ferramentas de análise de requisitos.

Existem ainda outros domínios que, não sendo nucleares da Engenharia Informática, são também muito relevantes e que se relacionam com os anteriormente indicados:

- **Segurança nas organizações**
  Este domínio implica conhecer e entender as principais ameaças, vulnerabilidades e riscos relacionados com a cibersegurança nas organizações e entender como uma organização pode desenvolver uma visão holística para suporte às atividades de governança, gestão e controlo da cibersegurança. Para tal são usadas ferramentas, um conjunto de boas práticas e fontes de informação relacionadas com a implementação de modelos e *frameworks* de segurança e políticas nos domínios organizacionais, processos, pessoas e tecnologias (ex. COBIT 5, NIST, SANS CIS *Critical Security Controls*, ISF, ISO/IEC 27002).
- **Conformidade e aspetos legais da cibersegurança**
  Por fim, este domínio considera os aspetos de conformidade legal e normativa relacionados como a segurança e cibersegurança nas organizações, nomeadamente: o cibercrime; enquadramento legal e normativo do digital nos contextos nacional, europeu e global; os desafios de gestão da privacidade da informação; a realização de auditorias (ex. forenses); processos de certificação em normativos internacionais relacionados com o risco, cibersegurança e continuidade/resiliência (e.g. EU's *Data Protection Directive*, ISO/IEC 27001:2013, PCI DSS, ISO 22301:2012).

Todos estes domínios, depois de bem assimilados e sendo aplicados, permitem garantir a segurança da informação, a segurança de aplicações, a segurança das redes de comunicação, a segurança na Internet, a segurança na nuvem, a segurança nas bases de dados e a proteção das infraestruturas críticas de informação e comunicação. É de notar que o conhecimento nos domínios atrás indicados é condição necessária mas não suficiente para garantir a cibersegurança. Com efeito, é absolutamente indispensável que estes sejam implementados no terreno, quer individualmente, quer nas organizações, e isso também depende de fatores organizacionais e comportamentais. Por exemplo, se numa organização é decidido manter um determinado sistema operativo sem que lhe sejam efetuadas atualizações automáticas (e.g., porque isso é incompatível com algumas aplicações desenvolvidas *in-house*), o conhecimento atrás mencionado permitir-nos-á perceber que os SIC estão vulneráveis mas, se nada for feito, é como se saíssemos de casa e deixássemos a porta aberta.

Muitos dos ataques que têm sido noticiados recentemente, alguns dos quais com impacto gravíssimo nas instituições afetadas, resultam: i) do desconhecimento, e/ou ii) da incapacidade de compreensão das vulnerabilidades existentes, e/ou iii) da não aplicação das respetivas soluções. Assim, uma vez detetado um evento em que estas vulnerabilidades são efetivamente exploradas por malware, muitos indivíduos e organizações optam por simplesmente "desligar tudo e esperar que passe". Ora, esta solução é obviamente inadequada porque pode ser demasiado tarde quando tal acontece (i.e., quando se desliga o SIC da Internet o *malware* já se instalou e se propagou nos equipamentos) e porque não é aceitável que os SIC fiquem indisponíveis, pois a sociedade atual depende de forma crítica de alguns dos serviços em causa. Note-se que, neste caso, se o que o atacante pretende é conseguir que o serviço fique de facto indisponível (*denial of service*), então o seu objetivo foi claramente conseguido.

Portanto, resta apenas investir de forma clara e decidida no conhecimento, quer por parte das organizações, quer por parte dos indivíduos. Este é o único caminho possível, tal como se verifica noutras áreas da Engenharia desde há muito tempo (e.g., na Engenharia Civil no que diz respeito à segurança de edifícios) e que, mais cedo do que tarde, se tornará inevitável por força da lei a que estamos obrigados pela UE. Com efeito, um bom exemplo desta obrigatoriedade resulta da legislação europeia que entrará em vigor no primeiro semestre de 2018, sobre a proteção dos dados pessoais (já antes referida). Esta lei obriga e responsabiliza de forma veemente as organizações que tendo na sua posse dados pessoais dos seus clientes/utilizadores/etc. não garantam a sua segurança. Ora, todos sabemos os inúmeros casos de roubo de informação pessoal como nomes, moradas, números de cartões de crédito, etc. A partir de 2018, se tal suceder as organizações serão exemplarmente penalizadas (e.g., multas elevadíssimas).

Assim, é indispensável que as organizações adquiram o conhecimento necessário na área da Engenharia Informática, em parti-

cular nos domínios da cibersegurança anteriormente mencionados. Para tal, é preciso capacitar os recursos humanos para que estes possam intervir no processo de decisão ao mais alto nível, tornando claro as vulnerabilidades resultantes de eventuais más decisões (e.g., manter versões desatualizadas dos sistemas operativos) e das respetivas consequências gravíssimas. Será também necessário assegurar que as decisões tomadas ao mais alto nível sejam de facto aplicadas atempadamente e de forma abrangente (bem sabemos que um sistema será tão fraco quanto mais fraco for um dos seus componentes, i.e., basta deixar uma janela aberta, apesar de todas as outras terem sido fechadas, para a vulnerabilidade ser total).

É também necessário que os utilizadores dos SIC, na sua vertente mais aplicacional, estejam cientes das suas responsabilidades aquando da utilização de certas aplicações, e.g., correio eletrónico, *browser*, etc. É verdade que algum do *malware* explora vulnerabilidades do muito *software* existente (sistema operativo, *middleware*, redes, etc.) mas alguns dos ataques bem-sucedidos dependem de comportamentos individuais cujas consequências são incompreendidas por estes. Por exemplo, quando um utilizador diz que "apenas abriu um ficheiro que recebeu em anexo a uma mensagem de correio eletrónico", ou que "seguiu um *link* no seu *browser*", desconhece os riscos que corre pois não tem conhecimento necessário para tal.

Numa organização, cabe a esta capacitar os seus recursos humanos para lidar com comportamentos de risco, e à sua equipa de Engenharia Informática – cibersegurança (em conjunto com as outras equipas, e.g. de gestão) aplicar todas as soluções ao seu alcance para impedir (ou minimizar) as consequências nefastas dos casos referidos. Ora, para que tal aconteça, é fundamental dispor do conhecimento respetivo nos domínios mencionados e que cobrem o *software* em todas as suas camadas, desde a de mais baixo nível (sistema operativo), até ao mais alto (aplicações), passando pela infraestrutura que se apoia na nuvem, nas redes e em bases de dados.

## 3. DESAFIOS NO HORIZONTE

Os desafios nesta área para as organizações são muitos e, como em qualquer área da Engenharia, estão em permanente evolução. A evolução tecnológica e o advento dos computadores quânticos poderão tornar obsoletos os algoritmos criptográficos atualmente em utilização e levarão ao aparecimento de novos paradigmas como a criptografia de reticulados. As próprias ameaças e potenciais atacantes também estão a evoluir com o tempo sendo neste momento possível a um utilizador sem grandes conhecimentos criar *ransomware* à medida utilizando serviços disponíveis para esse efeito. Para além disso, o número de dispositivos ligados em rede de forma não supervisionada (*Internet of Things*) cresce a cada dia que passa formando estes um exército digital para quem os conseguir controlar.

## 4. CONCLUSÕES

Considerando a crescente dependência das organizações dos SIC é hoje impensável que a cibersegurança não seja entendida como a segurança do negócio em si. Neste contexto é inegável o papel fundamental da Engenharia Informática no desenvolvimento da cibersegurança das organizações. Cabe aos engenheiros informáticos desempenhar um papel preventivo na conceção de sistemas, por forma a diminuir o número de vulnerabilidades criadas e consequentemente a exposição das organizações. No entanto, para a gestão contínua da cibersegurança das organizações, os engenheiros informáticos necessitam continuamente de reforçar as suas competências por forma a acompanharem a constante evolução dos desafios que esta área apresenta. É fundamental que os nossos recursos humanos estejam cada vez mais capacitados e sempre um passo à frente dos potenciais atacantes. Estratégias de defesa de perímetro serão cada vez mais ineficazes face aos atuais ataques dirigidos.

Um novo paradigma de educação focado na análise das vulnerabilidades das organizações é imperativo, por forma a olhar para esta da mesma forma que um atacante. Por outro lado, a transversalidade do conhecimento necessário a um profissional de cibersegurança é frequentemente apontada como um dos principais obstáculos à sua formação e um dos problemas que as escolas de Engenharia Informática têm que ultrapassar, no sentido de produzirem profissionais em número e qualidade suficiente às necessidades.

Na vertente da regulação da atividade em causa, cabe à sociedade regular a atividade de Engenharia Informática, tendo aqui a Ordem dos Engenheiros um papel central, responsabilizando os engenheiros pela conceção e manutenção destes sistemas complexos, fulcrais para a sobrevivência das organizações.

Por fim, é de notar que a cibersegurança não se resume às componentes tecnológicas e organizacionais, nas quais a Engenharia Informática participa ativamente. A cibersegurança envolve outras áreas de conhecimento, como o direito e a psicologia, sendo essencial uma abordagem sistémica na formação de todos os cidadãos, em todos os níveis de ensino, para lidar com esta nova realidade.