Conceitos e práticas para a cibersegurança como atividade do dia-a-dia

Gouveia, L. (2024). Conceitos e práticas para a cibersegurança como atividade do dia-a-dia. Webinário. FNE, Federação Nacional da Educação. 17 de outubro.

Conceitos e práticas para a cibersegurança como atividade do dia-a-dia

Não seja uma vítima – Seja mais inteligente do que um Hacker

*Vivemos um tempo em que o **mundo digital se interliga com o nosso mundo físico, o analógico**. Num contexto em que as fronteiras entre estes dois mundos se fundem e em que a nossa atividade quer de trabalho ou de lazer, é cada vez mais **uma fusão e um híbrido do físico e do digital**. Neste contexto, tal como nos preocupamos com fechar portas e guardar e acautelar os nossos bens, temos que o fazer também no contexto digital. Mais ainda, **proteger a informação que nos pode identificar ou que implique com as nossas atividades mais relevantes**.*

*No digital, em face das suas diferenças para o analógico, temos de entender conceitos e diferenças para as que habitualmente são as nossas práticas de segurança, de modo a estabelecer níveis mínimos de segurança também no mundo digital (**cibersegurança**).*

*Deste modo é proposta a partilha de um conjunto de conceitos sobre o tema da cibersegurança e de **boas práticas** que importa assegurar de modo **a mitigar os riscos existentes**, face à crescente sofisticação de ameaças com que temos de lidar. E sim, a inteligência artificial também neste contexto tem um papel a desempenhar.*

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Nota prévia

A celebração do conhecimento e o cuidado de ser ético, evitando o seu mau uso

Hackers

Gouveia, L. (2024). A componente humana na Segurança da Informação. Keynote. Digital Privacy and Security Conference 2024. VII Jornadas de Segurança Informática. 10 de Janeiro. Porto, Universidade Lusófona. https://bdigital.ufp.pt/handle/10284/12597

- *Hackers* são pessoas que se dedicam de forma apaixonada e intensa a solucionar problemas e criar soluções que envolvem tecnologia, computação e a informática
  - Podem ser ou não informáticos; podem ser ou não adultos
  - Podem ou não estar enquadrados institucionalmente
  - Muito associados a acessos indevidos e a contextos limite ou mesmo ilegais
  - o termo *hacker* surgiu na década de 1960 (EUA), com a expressão *hack* para designar uma solução inovadora e criativa para um qualquer problema que contenha conhecimento específico de computadores e redes (hardware e software)
- *Ethical hackers* (*white hat hackers*): não prejudicam o sistema ou organização e atuam de forma oficial e autorizada para explorar vulnerabilidades e penetrar nos sistemas, fornecendo soluções para os eventuais problemas que descubram e assim contribuir para o garantir da segurança

O contexto

*Vivemos um tempo em que o **mundo digital se interliga com o nosso mundo físico, o analógico**. Num contexto em que as fronteiras entre estes dois mundos se fundem e em que a nossa atividade quer de trabalho ou de lazer, é cada vez mais **uma fusão e um híbrido do físico e do digital**.*

Mundo digital

- *Complexo, dinâmico e imprevisível*
  +VUCA (volátil, incerto, complexo e ambíguo)
  + rápido
- *IA para ajudar e transformar*
- *Os dados valem*
- *Requer o acesso a recursos e ferramentas*
- *Requer conhecimento especializado*
- *Difícil de acompanhar*

Imagens criadas por LMBG, com a IA Bing Image Creator em Outubro de 2024

Novas literacias

- *Incontornável e difícil de evitar o uso de redes e computadores, da Internet, da Web e das plataformas digitais a que acedemos com a nossa identidade*

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Princípios

No digital, em face das suas diferenças para o analógico, temos de entender conceitos e diferenças para as que habitualmente são as nossas práticas de segurança, de modo a estabelecer níveis mínimos de segurança também no mundo digital

Dados e Ativos Digitais

- No centro da cibersegurança, estão os **dados e ativos digitais** (informação, sistemas, redes, dispositivos) que precisamos proteger

- **O que se deve proteger?**
  - Informação sensível (dados pessoais, financeiros, empresariais)
  - Infraestrutura digital (servidores, redes, dispositivos)

- Implica **elementos críticos**
  - um **email** (endereço de correio eletrónico)
  - uma **ID** (assinatura digital/cartão CC/passaporte)
  - um **dispositivo** (telemóvel/USB Key)

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Ameaças e Vulnerabilidades

- Os **riscos** vêm de ameaças (hackers, *malware*, vírus, etc.) e **vulnerabilidades** (falhas de software, erros humanos, má configuração)

- **De quem ou de quê nos estamos a defender?**
  - Hackers (ameaças externas)
  - Colaboradores descuidados ou mal-intencionados (ameaças internas)
  - Ataques automatizados (vírus, *worms*)

Confidencialidade, Integridade e Disponibilidade (Tríade CIA)

- O objetivo da cibersegurança é garantir:
  - **Confidencialidade**: apenas pessoas autorizadas podem aceder a dados sensíveis
  - **Integridade**: os dados não podem ser alterados ou corrompidos sem autorização
  - **Disponibilidade**: os dados e sistemas devem estar acessíveis para uso legítimo sempre que necessário

- **Como proteger os ativos digitais?**
  - Proteger do acesso não autorizado (**Confidencialidade**)
  - Assegurar que os dados permaneçam precisos e completos (**Integridade**)
  - Garantir que os sistemas estejam sempre disponíveis (**Disponibilidade**)

Mecanismos de Defesa

- Para implementar a tríade CIA, são utilizadas **ferramentas e técnicas de defesa**:
  - **Criptografia**: para proteger a confidencialidade
  - **Assinaturas digitais e controlos de versão**: para proteger a integridade
  - **Backups e redundância de sistemas**: para garantir a disponibilidade

- **Quais os mecanismos que podem ser usados para garantir níveis de segurança?**
  - Firewall, criptografia, sistemas de deteção de intrusão (IDS), entre outros

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Gestão de Risco

- Não é possível eliminar todos os riscos, potenciais quebras de segurança podem sempre ocorrer
- Então a cibersegurança tem de assegurar a **gestão de risco** de forma eficiente

- **Como equilibrar o custo da proteção com o valor dos ativos?**
  - Avaliar e priorizar riscos (qual o risco é mais crítico?)
  - Implementar medidas de controlo baseadas na criticidade dos ativos

Elemento Humano

- As pessoas são tanto a primeira linha de defesa quanto o elo mais fraco

- **Como sensibilizar e treinar as pessoas para minimizar erros e aumentar a segurança?**
  - Políticas de senha forte, sensibilização sobre ameaças como o *Phishing* e a engenharia social

O que fazer?

Que atitude a ter para com os ativos de informação, como assegurar as práticas relacionadas com os cuidados a tomar, assegurando que a atividade do dia a dia não é comprometida ou subalternizada em função das medidas a tomar, para a segurança da informação

Um mapa para a ação

- Entender o que precisa de ser protegido (**informação e sistemas**)
- Compreender quais as **ameaças** a considerar (*hackers*, *malware*, falha humana)
- Usar a tríade CIA para garantir a **proteção** da informação
- Implementar mecanismos de **defesa** (criptografia, *firewalls*)
- Gerir os **riscos** tendo em consideração as ameaças que são mais críticas (com maior impacto)
- **Educar** todos os envolvidos, tendo em consideração que os erros humanos são inevitáveis, mas podem ser minimizados (mitigados)

Desenvolvendo

Entender o que precisa de ser protegido (dados e sistemas)

A base de qualquer sistema de cibersegurança é saber o que está ser protegido

- **Identificar Ativos**: começar por listar todos os ativos digitais da organização ou do indivíduo, como:
  - **Dados**: pessoais, financeiros, médicos, empresariais e outros que sejam críticos
  - **Sistemas**: servidores, computadores, dispositivos móveis, aplicações
  - **Infraestrutura**: redes, *data centers*, serviços na nuvem (plataformas digitais)
- **Classificação de dados**: nem todos os dados têm o mesmo valor. Os mais sensíveis exigem uma proteção diferenciada
  - **Exemplo**: testes e enunciados de exame tem mais sensibilidade que listas de exercícios ou separar testes de escolha múltipla da chave da sua resolução…
- Devemos compreender que **não é possível proteger tudo igualmente**. É preciso criar prioridades com base no valor e sensibilidade nos ativos a proteger e considerar estes com maior atenção (o **onde** e o **como** a informação é **armazenada**, **processada** e **comunicada**)

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Compreender quais as ameaças a considerar (hackers, malware, falha humana) conhecer as **ameaças e vulnerabilidades** que podem comprometer os ativos

- **Ameaças Externas**
  - **Hackers e Criminosos Cibernéticos**: pessoas mal-intencionadas que tentam roubar, corromper ou destruir dados
  - **Malware**: Software malicioso como vírus, *ransomware*, trojans, *worms*
  - **Ataques de *Phishing***: e-mails ou sites falsos que enganam os utilizadores para revelar senhas ou dados sensíveis (tipos de ataques *Phishing*: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks)
- **Ameaças Internas**
  - **Pessoas mal-intencionados**: pessoas dentro da organização que abusam do seu acesso
  - **Erros Humanos**: configurações incorretas, partilha acidental de informação sensível, uso de senhas fracas
- **Vulnerabilidades**
  - **Software desatualizado**: sistemas com falhas de segurança conhecidas
  - **Má configuração de sistemas**: como *firewalls* mal configurados ou permissões de acesso excessivas, ou ainda manter senhas de acesso por defeito em aplicações de sistema e de configuração
- Compreender estas ameaças é essencial para saber **o que deve ser prevenido e o como**

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Usar a tríade CIA para garantir a proteção dos dados

A tríade **Confidencialidade, Integridade e Disponibilidade (CIA)** é a base de uma estratégia de cibersegurança

- **Confidencialidade**
  - Garantir que apenas pessoas autorizadas podem aceder a informação sensível
  - **Como proteger**: uso de criptografia para proteger dados em trânsito e em repouso, autenticação forte (ex: autenticação de dois fatores)
- **Integridade**
  - Garantir que os dados não sejam alterados de forma não autorizada ou acidental
  - **Como proteger**: uso de assinaturas digitais e controlos de versão para detetar e impedir modificações não autorizadas
- **Disponibilidade**
  - Garantir que os dados e sistemas estejam disponíveis para uso quando necessário
  - **Como proteger**: implementação de backups regulares, redundância de servidores e mitigação de ataques DDoS (ataques de negação de serviço)
- A tríade CIA ajuda a garantir que os dados estejam **seguros, intactos e acessíveis**

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Implementar mecanismos de defesa (criptografia, firewalls)

Compreendidos os princípios e as ameaças, é o momento de aplicar as **ferramentas e técnicas** adequadas

- ***Firewalls***
  - Controlam o tráfego de rede, bloqueando acessos não autorizados e filtrando dados maliciosos
- **Criptografia**
  - Transforma dados sensíveis em um formato ilegível para quem não tem a chave de acesso
  - Usada tanto para proteger dados em repouso (armazenados) quanto em trânsito (enviados pela rede, em comunicação)
- **Sistemas de Deteção de Intrusão (IDS)**
  - Monitorização de atividades suspeitas e deteção de tentativas de acesso não autorizado
- **Controlo de Acessos**
  - Permite que apenas utilizadores autorizados possam aceder a certos recursos ou dados, bde acordo com os respetivos níveis de permissão
- **Autenticação Multifatorial (MFA)**
  - Exige múltiplas formas de verificação (como senha e um código enviado para o telemóvel) para permitir o acesso.
- Mecanismos a implementar com base no nível de risco e criticidade dos ativos que precisam de proteção

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Gerir os riscos tendo em consideração quais as ameaças mais críticas

- A gestão de risco é um aspeto essencial da cibersegurança, já que **não é possível eliminar todos os riscos**. O objetivo é **mitigar os mais graves**.
- **Avaliação de Risco**:
  - Identificar e quantificar os riscos mais prováveis e mais prejudiciais.
  - **Perguntas chave**: Qual seria o impacto de um ataque? Qual é a probabilidade de acontecer?
- **Priorização de Riscos**:
  - Riscos que têm um grande impacto, mesmo que sejam de baixa probabilidade, geralmente exigem atenção prioritária.
- **Mitigação de Riscos**:
  - Implementar controles ou medidas de proteção com base na criticidade.
  - **Exemplo**: Implementar criptografia para proteger dados financeiros críticos e monitoramento contínuo de atividades suspeitas.
- A estratégia de risco é garantir que os recursos da organização sejam usados da forma mais eficaz, investindo mais na proteção de ativos mais valiosos.

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Educar as pessoas, atendendo que os erros humanos são inevitáveis, mas podem ser minimizados

O **fator humano** é uma das maiores vulnerabilidades em cibersegurança. A consciência dos riscos, a sensibilização e o treino são essenciais para mitigar esse risco

- **Treino Regular**
  - Ensinar aos utilizadores práticas seguras, como:
    - Criação de senhas fortes e exclusivas
    - Reconhecimento de e-mails de *phishing*
    - Evitar o uso de redes públicas para atividades sensíveis
- **Políticas de Segurança**
  - Implementar políticas claras sobre o uso de dispositivos e redes, como:
    - Exigir a troca regular de senhas
    - Estabelecer diretrizes para o acesso remoto seguro
- **Simulações de Ataques**
  - Realizar simulações de ataques (como *phishing*) para educar os envolvidos e testar a resiliência da organização
- Educar e treinar as pessoas cria uma **primeira linha de defesa** que pode prevenir muitos dos erros humanos comuns que levam a violações de segurança

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Discussão...

Recursos para explorar

Instituições, cursos e informação sobre como reportar incidentes e crimes informáticos. Sugestão de algumas ferramentas em função das questões colocadas

Instituições nacionais e contrapartes europeias, relacionadas com a Cibersegurança

- **Centro Nacional de Cibersegurança** (CNCS) https://www.cncs.gov.pt/
  - ENISA: *https://www.enisa.europa.eu/*
- **CERT.PT** (equipa de resposta a incidentes de cibersegurança nacional) *https://www.cncs.gov.pt/pt/certpt/*
  - CERT.EU: *https://cert.europa.eu/*
- R**NCSIRT** (partilha de informação de carácter operacional) *www.redecsirt.pt*
- **Polícia Judiciária** (unidade nacional de combate ao cibercrime) *https://www.policiajudiciaria.pt/unc3t/*
- **Gabinete do Cibercrime** (Ministério Público) *https://cibercrime.ministeriopublico.pt/destaque/relatorio-ciberseguranca-em-portugal-0*

Alguns dos cursos sem custo que se podem frequentar na NAU

- Gestão dos Riscos de Cibersegurança nas Organizações *https://www.nau.edu.pt/pt/curso/gestao-dos-riscos-em-ciberseguranca-nas-organizacoes/*
- Cidadão Cibersocial *https://www.nau.edu.pt/pt/curso/cidadao-cibersocial/*
- Informação: Cópias de Segurança, Armazenamento e Destruição *https://www.nau.edu.pt/pt/curso/informacao-copias-de-seguranca-armazenamento-e-destruicao/*
- Cidadão Ciberseguro *https://www.nau.edu.pt/pt/curso/cidadao-ciberseguro/*
- Consumidor Ciberseguro *https://www.nau.edu.pt/pt/curso/consumidor-ciberseguro/*
- Cidadão Ciberinformado *https://www.nau.edu.pt/pt/curso/cidadao-ciberinformado/*

Ferramentas…

- **Gerador de Palavras-Passe Aleatórias**
  https://www.avast.com/pt-pt/random-password-generator
  - Os hackers não invadem: eles fazem login *https://support.google.com/chrome/answer/95606*
- Para guardar palavras-passe (**Navegador Google Chrome**) *https://support.google.com/chrome/answer/95606*
  - Lastpass – **Gestor de passwords**, extensão do Chrome: *https://chromewebstore.google.com/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd*
- **Antivírus gratuitos**
  - AVG: *https://www.avg.com/pt-pt/*
  - AVAST*:* *https://www.avast.com/pt-pt*
  - Bitdefender: *https://www.bitdefender.com/*
  - Avira: *https://www.avira.com/*
- **Encriptar dados** (proteger o acesso à informação)
  - BitLoker (Ferramenta MS Windows): *http://windows.microsoft.com/pt-br/windows7/products/features/bitlocker*
  - DiskCryptor (para encriptar áreas de volumes, memória secundária): *https://diskcryptor.net/*
  - AxCrypt (equivalente ao diskcryptor mas para ficheiros): *http://www.axantum.com/axcrypt/*
  - *AESCrypt (ferramenta leve para encriptar um ficheiro específico)* *https://www.aescrypt.com/windows_aes_crypt.html*
  - *MiniLock (associa chaves públicas além de encriptar os ficheiros):* *https://minilock.io/*
- IDS, **Sistemas de Deteção de Intrusão**
  - Suricata: *https://suricata.io/*
  - Security Onion: *https://securityonionsolutions.com/*
- **Teste a redes Wi-FI** (redes sem fios)
  - Ekahau (pontos de acesso existes e força de sinal): *https://www.ekahau.com/solutions/wi-fi-heatmaps/*
  - InSSIDer (informação sobre as redes disponíveis): *https://www.metageek.com/inssider/*
  - Wireshark (analisador de protocolos): *https://www.wireshark.org/*

E ainda…

Nunes, V. (2012). A definição de uma Estratégia Nacional de Cibersegurança. 133(5), 113-127. Revista Nação e Defesa.
https://comum.rcaap.pt/bitstream/10400.26/42467/1/Nunes_PauloViegas_A%20defini%C3%A7%C3%A3o%20de%20uma%20estrat%C3%A9gia%20nacional%20de%20ciberseguran%C3%A7a_NeD133_p_113_127.pdf

- Observatório de Cibersegurança
  https://www.cncs.gov.pt/pt/observatorio/
- Estratégia nacional de Segurança no Ciberespaço
  https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf
- A componente militar da cibersegurança – Ciberdefesa
  https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa
- **Como reportar um incidente de forma voluntária (CNCS)**
  https://www.cncs.gov.pt/pt/como-reportar-um-incidente/
  (a comunicação não substitui queixa à autoridade judiciária ou ao órgão de polícia criminal quando os incidentes configurem um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular)
  - **Polícia Judiciária, PJ**: unc3t@pj.pt
  - **Procuradoria-Geral da República, PGR**: cibercrime@pgr.pt
- *Sobre a lei do cibercrime* ***o que fazer em caso de se ser vítima de um crime informático***
  - CGD: *https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/lei-do-cibercrime.aspx*

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Luis Borges Gouveia

Dip (UPT), MsC (FEUP), PhD (ULANCS), PD (FLUP) http://homepage.ufp.pt/lmbg

Os seus interesses estão relacionados com o digital e como o seu uso e exploração pode beneficiar indivíduos e organizações, nomeadamente nas questões associadas com o ensino e aprendizagem, com a segurança da informação e a IA

Professor Catedrático da Universidade Fernando Pessoa (**UFP**)
https://www.ufp.pt/

Membro Integrado do grupo Informação, Comunicação e Cultura Digital do **CITCEM**, FLUP
https://citcem.org/

Colaborador do LIACC, Laboratório de Inteligência Artificial e Ciência de Computadores, FEUP
https://liacc.fe.up.pt/

Sócio e Membro da Direção da Delegação Norte da **APDSI** (ONG que promove a discussão do digital e de como promover uma sociedade mais capaz de lidar com o digital)
https://apdsi.pt/

UIDB/04059/2020