# FICHA TRABALHO 1

| | | | |
|---|---|---|---|
| MODALIDADE: | Aprendizagem + | Não aplicável | |
| CURSO: | Técnico/a Especialista em Gestão de Informação e Ciência dos Dados | | |
| UFCD: | Segurança no desenvolvimento do software | CÓDIGO UFCD: | 10795 |
| FORMADOR/A: | Bruno Silva | DATA: | |

OBJETIVOS

- Instalação e configuração ao mundo da criptografia e PGP (pretty good privacy)

## 1.1 – O que é cibersegurança?

Segurança cibernética é o esforço contínuo para proteger indivíduos, organizações e governos contra ataques digitais, protegendo os sistemas e dados em rede contra uso não autorizado ou danos em pontos específicos.

Vamos ver com mais detalhe cada uma das 3 áreas enunciadas mais acima

- ***Nível pessoal:*** a nível pessoal, você precisa proteger a identidade, os dados e os dispositivos de computação.



- ***Nível organizacional:*** a nível organizacional, é responsabilidade de todos proteger a reputação, os dados e os clientes da organização.



- ***Nível governamental:*** À medida que mais informação digital é recolhida e partilhada, a sua proteção torna-se ainda mais vital a nível governamental, onde estão em jogo a segurança nacional, a estabilidade económica e a segurança e o bem-estar dos cidadãos.



## 1.2 – Os nossos dados pessoais

Os dados pessoais descrevem qualquer informação sobre nós, incluindo o nome, número do segurança social, número de contribuinte, data e local de nascimento, estado civil e até fotos ou mensagens enviadas para familiares e amigos.




Os ***criminosos virtuais*** podem usar essa informação valiosa para identificar e passar por nós, violando a nossa privacidade e causar vários problemas. ***Isto vai fazer pensar um pouco... Vamos ver alguns exemplos!***

***Exemplo 1: Viagens e compartilhamento de imagens***

- Fizeram uma viagem ao Dubai. De seguida, compartilhou algumas fotos do telemóvel com os amigos mais próximos.
- ***Nota importante:*** as fotos estão apenas no vosso telemóvel.

• Neste caso, compartilhou as fotografias com cinco amigos próximos, que moram em vários locais do mundo.





• De seguida, todos os amigos baixaram as fotos e agora têm cópias das fotos nos dispositivos.

- Um dos amigos ficou tão fascinado com uma imagem que decidiu publicar e compartilhar as suas fotos.

***Resumindo:*** As fotos já não estão apenas no dispositivo pessoal. Na verdade, estas fotos acabaram por ser replicadas em servidores e em diferentes partes do mundo e pode haver outras pessoas (que nem sequer conhecemos) têm acesso às vossas fotos.

Este é apenas um exemplo que faz lembrar que toda vez que compartilhamos dados pessoais, devemos considerar a nossa segurança. Existem diferentes leis que protegem a privacidade e os dados no nosso país. Mas sabem onde estão os vossos dados?

***Vejamos exemplos que podem não ser tão óbvios....***

***Exemplo 2: Saúde e seguradoras***

- Após uma consulta, o médico atualizará a ficha médica e será feita a faturação da consulta.
- Para efeitos de cobrança, essas informações podem ser compartilhadas com a empresa de seguros para garantir a qualidade e a cobrança adequadas.
- Nesses casos, parte da informação médica pode ser acedido pela seguradora.

***Exemplo 3: Cartões de fidelidade***

- Os cartões de fidelidade das lojas podem ser uma maneira conveniente de guardar dinheiro para as nossas compras.
- No entanto, a loja está a usar este cartão para criar um perfil e saber o vosso comportamento de compras e pode ser usado para direcioná-lo com ofertas especiais de acordo com os parceiros de marketing

## 1.3 – Dispositivos inteligentes

**Considerem com que frequência usam os dispositivos digitais para aceder aos dados pessoais?**

- A menos que tenha optado por receber extratos em papel, hoje em dia é quase preferível aceder as cópias dos documentos digitais ou extratos por meio de uma plataforma digital.
- E ao pagar uma conta, é altamente provável que tenham transferido os fundos necessários por meio de uma plataforma digital (tablet, smartphone, etc ...).
- Estes dispositivos, para além de permitir aceder as informações, também podem gerar informações sobre nós.
- Tecnologias versáteis, como smartwatches e os dispositivos de localização de atividades, coletam os nossos dados para pesquisas clínicas, monitoramento da saúde do paciente e bem-estar.

- À medida que o mercado global dos dispositivos de localização de fitness cresce, também aumenta o risco para os seus dados pessoais.
- Analisando mais a fundo, não devemos esquecer que estes dispositivos podem estar interligados num ecossistema (tablets, telemóveis, smartwatches, ...) e todos estes terem acesso a informação que é recolhida por um destes elementos.



***Sabiam que....***

- ***Pode parecer que a informação disponível online é gratuita. Mas será a privacidade o preço que pagamos por esta conveniência digital?***
- Por exemplo, as empresas de redes sociais geram a maior parte do seu rendimento através da venda de publicidade direcionada com base em dados de clientes que foram extraídos através de algoritmos ou fórmulas. É claro que essas empresas argumentarão que não estão "vendendo" dados de clientes, mas "compartilhando" dados de clientes com seus parceiros de marketing.

## 1.4 – O que é que os Hackers querem?

Os cibercriminosos são certamente muito criativos quando se trata de obter acesso ao nosso dinheiro. Mas não é só isso que procuram – também podem roubar a nossa identidade e arruinar a vida para fins ilícitos.



O aumento dos custos médicos também levou a um aumento no roubo de informações sobre seguros médicos para usar os benefícios para si próprios.

Quando isso acontecer, quaisquer procedimentos médicos realizados serão salvos nos vossos registos médicos (quando na realidade foram outras pessoas).




O roubo de dados privados pode ajudar os cibercriminosos a aceder a contas bancárias, cartões de crédito, perfis sociais e outras contas.

Com essas informações, um ladrão de identidade poderia apresentar uma declaração de impostos falsa e receber o vosso reembolso. Mas, também contrair empréstimos no vosso nome.



## 1.5 – Ciberespaço

Nos últimos anos deu-se um crescimento verdadeiramente explosivo das tecnologias de informação, nomeadamente da Internet.

Na sequência desta expansão, o termo ciberespaço passou a descrever o mundo virtual que os utilizadores da Internet visitam quando estão online, acedendo aos mais diversos conteúdos que a rede mundial de computadores disponibiliza.

Mas é fundamental distinguir o ciberespaço da infra-estrutura física das redes de comunicação, pois existe uma confusão conceptual.

As telecomunicações e a informática, a chamada telemática, limitam-se a permitir a comunicação à distância, enquanto o ciberespaço é um ambiente virtual que se serve destes meios de comunicação para o estabelecimento de relações virtuais.

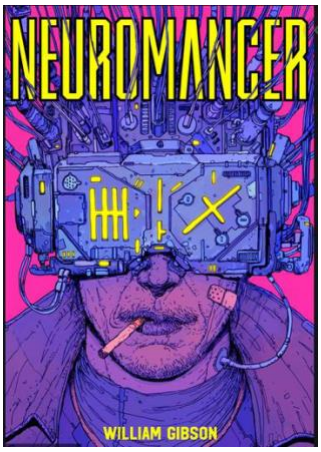


## 1.6 – Cibercrime

Cibercrime pode ser definido como qualquer crime que seja cometido por meio de computadores, redes de computadores ou outras formas de tecnologia de comunicação da informação.

***Origem do termo:***

- Termo criado em 1982 por William Gibson;
- Monitores de laptop, telemóvel, tv, são o acesso ao ciberespaço, constituído por circuitos e impulsos eletrónicos;
- Um espaço para novas práticas sociais, novas formas de viver e conviver;
- Experiências vividas são quase reais, intensas e atraentes;




***Exemplos de cibercrimes:***

- Atividades como a criação e disseminação de conteúdos maliciosos;
- Roubar dados pessoais ou industriais confidenciais;
- Ataques de negação de serviço para causar danos financeiros e/ou reputacionais;
- Burlas online;
- Cyberbullying ou discursos de ódio;

***Ameaças cibernéticas:***

CIO from IDG
Segurança da informação será prioridade no pós-pandemia ...
... o estudo confirma o protagonismo da segurança cibernética durante ... Que novas ameaças cibernéticas surgiram e em que grau elas estão ...
1 week ago



https://www.tecmundo.com.br
Ransomware, busca de senhas e roubo de informações: as principais ameaças cibernéticas de 2020 nomeadas
«Em 2020, houve um grande aumento nas ameaças, cujos motivos podem ser ... o número de ataques cibernéticos cresceu, sua complexidade aumentou e ...
3 weeks ago



Gizmodo Brasil
Ataque hacker que mirou Windows, Android e iOS partiu de ...
... efetivamente encerrou uma missão cibernética de "contraterrorismo ao ... Qual era a ameaça de "terror" que eles estavam investigando?
12 hours ago



Consultor Jurídico
Comitê apresenta protocolos de segurança cibernética para ...
O Comitê de Segurança Cibernética do Poder Judiciário concluiu a ... As crescentes ameaças de ataques cibernéticos, problema que afeta a ...
2 weeks ago



https://www.tecmundo.com.br
Vulnerabilidade de ataque de hacker por meio do Microsoft Exchange Server ameaça nova crise de segurança...
... do Microsoft Exchange Server ameaça nova crise de segurança cibernética. Ad ... atual pode se transformar em uma "crise de segurança cibernética global".
3 weeks ago



VEJA.com
Hackers invadem sistema da Microsoft e fazem 60 mil vítimas no mundo
Ataque ao software de e-mail reacende debate sobre segurança cibernética; Casa Branca pede atenção e diz que ameaça ainda está ativa.
3 weeks ago

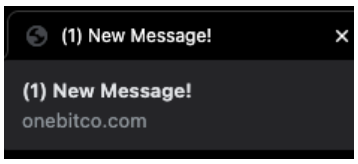


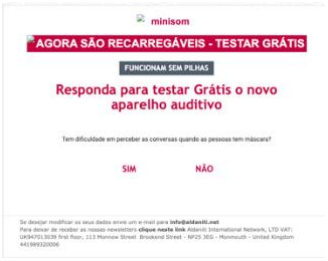
Sputnik Brasil
Hackers obtêm dados de funcionários do Departamento de Segurança Interna dos EUA, diz mídia
... de funcionários de segurança cibernética do departamento, diz mídia. ... cujo trabalho incluía a procura de ameaças de países estrangeiros, ...
19 hours ago




Valor Econômico
Empresas lançam soluções voltadas a riscos cibernéticos
Ameaças digitais estão em segundo lugar no ranking de preocupações de CEOs no mundo. Por Martha Funke — Para o Valor, de São Paulo. 25 ...
5 days ago








## 1.7 – Ciberterrorismo

Uso da Internet para realizar atos violentos que resultam em, ou ameaçam, perda de vidas ou danos corporais significativos, a fim de obter ganhos políticos ou ideológicos por meio de ameaça ou intimidação.

## 1.8 – Ciberespionagem

Espionagem efetuada com recurso a meios informáticos, uso de computadores, redes de telecomunicações e/ou outras tecnologias de informação para recolha de informação confidencial.

## 1.9 – Hacking e tipo de ataque

Método de ataque por um invasor ou grupos de invasores que invadem sistemas ou redes de computadores para obter acesso às informações.

Estes podem ser classificados de várias formas, pois, nem todos os hackers devem ser associados a atividades criminosas.

Em termos de tipos de ataques, ***podemos classificar por 3 grupos***:



***Amadores***



***Hackers***



***Organizações de hackers***

### 1.9.1 – Amadores

Refere-se a hackers amadores ou inexperientes que usam ferramentas ou instruções existentes encontradas na Internet para lançar ataques (embora que utilizem ferramentas básicas, os ataques podem ter consequências devastadoras);



## 1.9.2 – Hackers

Este grupo de invasores invade sistemas de computadores ou redes para obter acesso. Dependendo da intenção da invasão, estes podem ser classificados como:

- hackers de chapéu branco (***White hat attackers***);
- hackers de chapéu cinza (***Gray hat attackers***);
- hackers de chapéu preto (***Black hat attackers***);



***White hat attackers:*** Hackers que invadem redes ou sistemas de computadores para identificar pontos fracos na segurança dos sistemas ou na rede para depois melhorar. Essas invasões são feitas com permissão prévia e quaisquer resultados são relatados ao proprietário.

***Grey hat attackers:*** Hackers que tentam encontrar vulnerabilidades num sistema, mas só reportam as descobertas aos proprietários de um sistema se isso coincidir com os objetivos. Ou podem até publicar detalhes sobre a vulnerabilidade na Internet para que outros invasores possam explorá-la.

***Black hat attackers:*** Hackers que aproveitar qualquer vulnerabilidade para obter ganhos pessoais, financeiros ou políticos ilegais, com o objetivo de usar essas informações a seu favor para as mais diversas situações.

- ***Muito ligado ao termo <u>Ciberterrorismo</u>***

## 1.9.3 – Organizações de hackers

Estes invasores incluem organizações de criminosos cibernéticos, hacktivistas e terroristas para recolher informações ou cometer sabotagens.

Geralmente, estes hackers são altamente sofisticados e organizados e podem até fornecer o crime cibernético como um serviço a outros criminosos.



## 1.10 – Vantagens e desvantagens do ciberespaço

### 1.10.1 – Vantagens

- ***1 - Recursos Informativos***
    - É uma biblioteca virtual de informações. Podem obter qualquer tipo de informação sobre qualquer assunto do seu interesse. Para auxiliar as consultas de informação, existem motores de busca como Google e estão ao nosso serviço 24 horas por dia e 7 dias por semana.
- ***2 – Comunicação***
    - No passado, para comunicar com alguém teria que ligar para essa pessoa ou enviar uma carta pelo correio. Com a introdução da Internet, agora podemos enviar e receber mensagens por correio eletrônico instantaneamente e sem a necessidade de um selo postal.
- ***3 – Redes Sociais***
    - As redes sociais também desempenham um papel importante no ciberespaço.
    - Tornou-se tão popular entre os jovens e tem sido uma dependência tecnológica na vida quotidiana que um dia pode substituir a rede física.
- ***4 – Entretimento***
    - Com a Internet é possível descarregar informação como jogos, filmes e músicas em vez de sair da sua zona de conforto para obter o jogo ou CD mais recente numa loja física. Existem vários jogos que podem ser baixados gratuitamente. Graças a isso, a indústria dos jogos online cresceu drasticamente.
- ***5 – Oportunidades***
    - Além de encontrar amigos há muito perdidos, também pode procurar emprego, oportunidades de negócios, comunidades, etc. Além disso, existem salas de chat onde os utilizadores podem conhecer novas pessoas.

## 1.10.2 – Desvantagens

- ***1 – Segurança Comprometida***
    - Se usam a Internet para serviços bancários online, redes sociais ou outros serviços, corre o risco de roubarem as vossas informações pessoais, como nome, endereço, número de cartão de crédito, etc.
- ***2 – Ataques de Malware***
    - Os utilizadores da Internet são frequentemente atormentados por ataques de vírus através de múltiplas formas (ficheiros, imagens, hiperligações, entre outros métodos).
- ***3 – Cibercrimosos***
    - Infelizmente, a capacidade de enviar e receber emails, também criou um meio para os cibercriminosos distribuírem spam e malware . Malware escondido em anexos de um mail pode causar estragos nos nossos sistemas ou possivelmente até mesmo criar uma porta dos fundos (backdoor) para que um invasor infiltre no sistema (sem que os utilizadores apercebam disso).
- ***4 – Corrupção ativa e passiva***
    - Por meio de e mails, os cibercriminosos viram isso como mais uma oportunidade de brincar com as emoções humanas e induzir as vítimas a revelar informações confidenciais por meio de golpes de phishing
- ***5 – Roubo de identidade***
    - Pessoas mal intencionadas podem aceder a essas informações por meio de conexões não seguras ou introduzindo software e então obter os nossos dados pessoais e usar para atos maliciosos.

## 1.11 – Centro Nacional de Cibersegurança (CNCS)

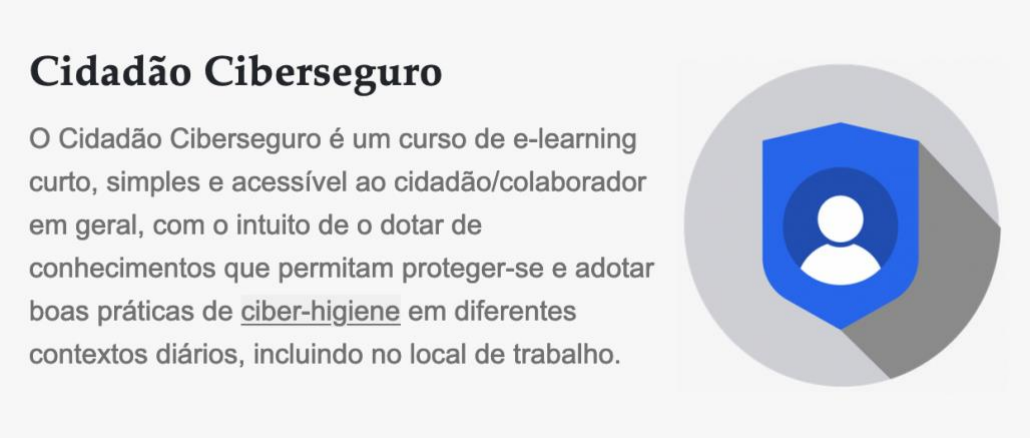
O Centro Nacional de Cibersegurança atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de Infraestruturas Críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático.

***Missão da Entidade:***

"Contribuir para que Portugal use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurançanacional e da cooperação internacional."

O CNCS promove a divulgação dos conhecimentos técnicos, táticos e estratégicos de cibersegurança necessários para o seguro funcionamento das entidades do Estado, dos operadores de serviços essenciais e dos prestadores de serviços digitais, bem como perspetivas substanciadas de ação para a implementação de medidas de cibersegurança.

## Programas de Informação e cibersegurança CNCS



## Cidadão Ciberinformado

O curso de e-learning Cidadão Ciberinformado destina-se a qualquer cidadão que procure aprender a identificar notícias falsas e a verificar a veracidade da informação consultada online, evitando a partilha de desinformação e contribuindo para um ciberespaço verdadeiramente democrático.



## Consumidor Ciberseguro

Através do curso de e-learning Consumidor Ciberseguro os formandos poderão obter conhecimentos que lhes permitam proteger-se e adotar boas práticas quando realizam compras online, evitando de modo mais eficaz a burla e o roubo de credenciais de cartões de crédito, por exemplo. Com este curso cada um poderá fazer compras online com mais segurança.



## Cidadão Cibersocial

O curso de e-learning Cidadão Cibersocial é uma iniciativa do Centro Internet Segura, coordenado pelo Centro Nacional de Cibersegurança. Trata-se de um curso interativo, que procura ser apelativo para todas as pessoas que queiram saber como utilizar as redes sociais de um modo mais seguro e protegendo a sua privacidade.



Recursos para Sensibilização do CNCS e o programa Cidadão Ciberseguro: https://www.cncs.gov.pt/pt/recursos-para-sensibilizacao