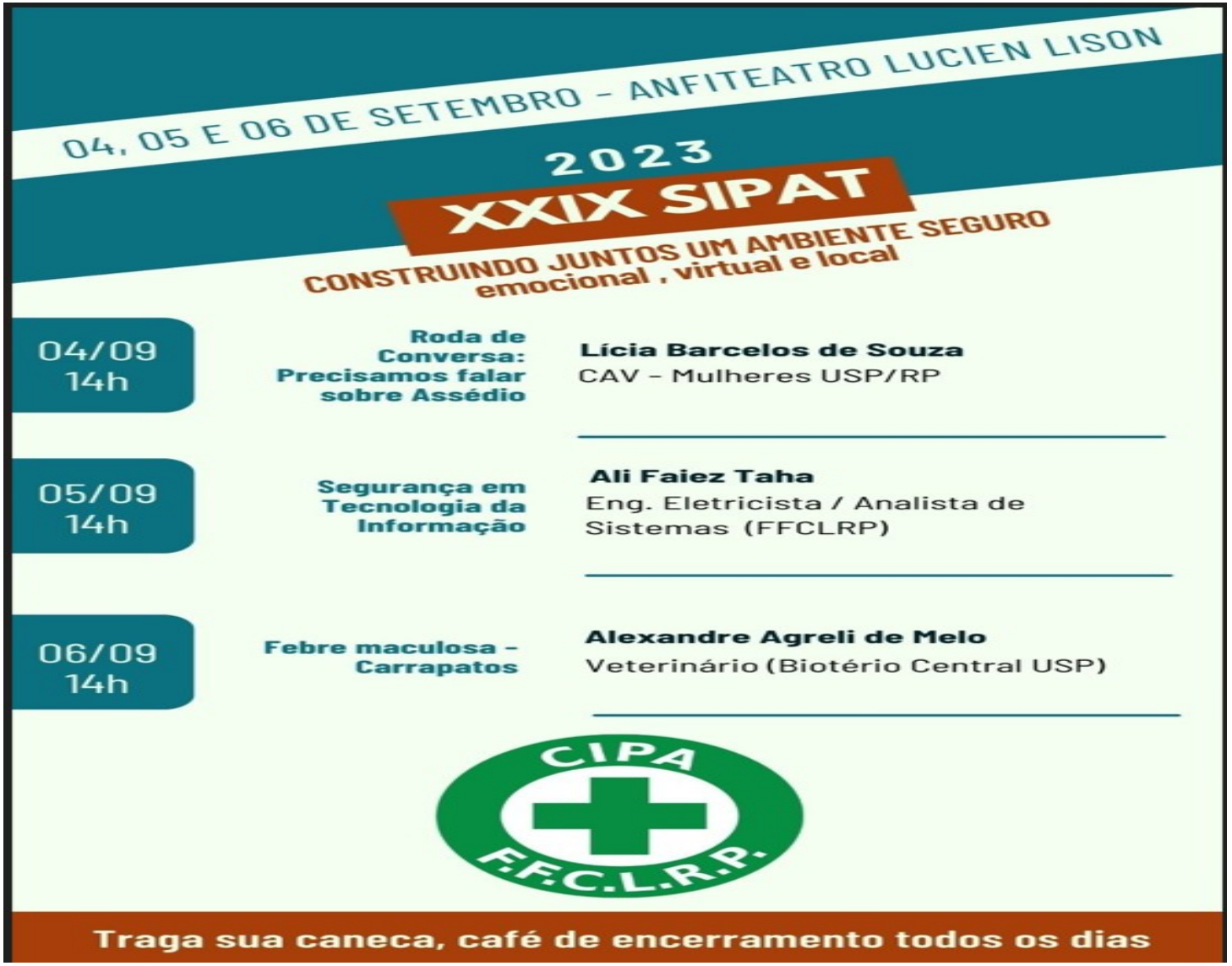
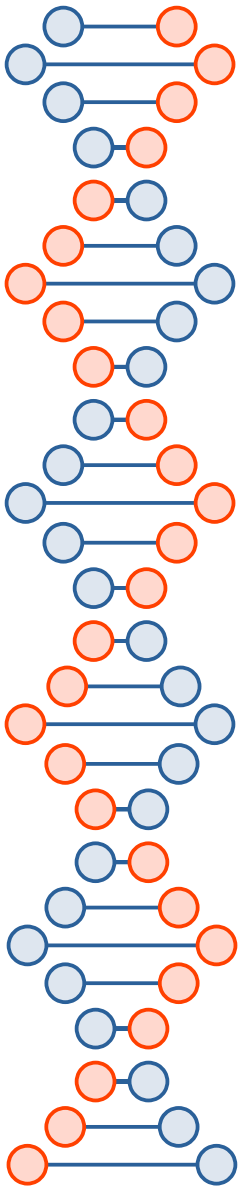
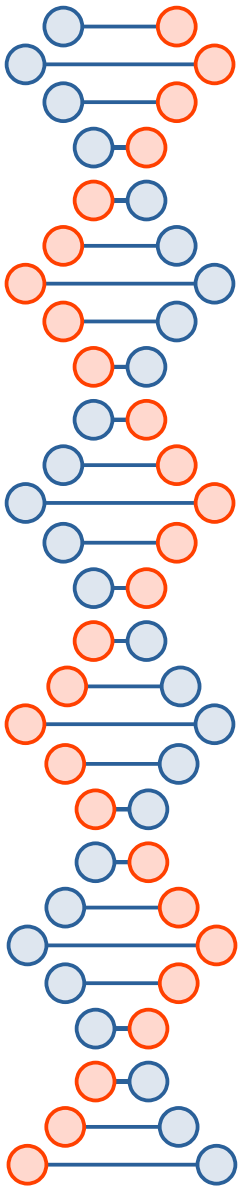

04, 05 E 06 DE SETEMBRO – ANFITEATRO LUCIEN LISON
2023
XXIX SIPAT
CONSTRUINDO JUNTOS UM AMBIENTE SEGURO
emocional , virtual e local
04/09
14h
Roda de Conversa: Precisamos falar sobre Assédio
Lícia Barcelos de Souza
CAV – Mulheres USP/RP
05/09
14h
Segurança em Tecnologia da Informação
Ali Faiez Taha
Eng. Eletricista / Analista de Sistemas (FFCLRP)
06/09
14h
Febre maculosa – Carrapatos
Alexandre Agreli de Melo
Veterinário (Biotério Central USP)
CIPA
F.F.C.L.R.P.
Traga sua caneca, café de encerramento todos os dias



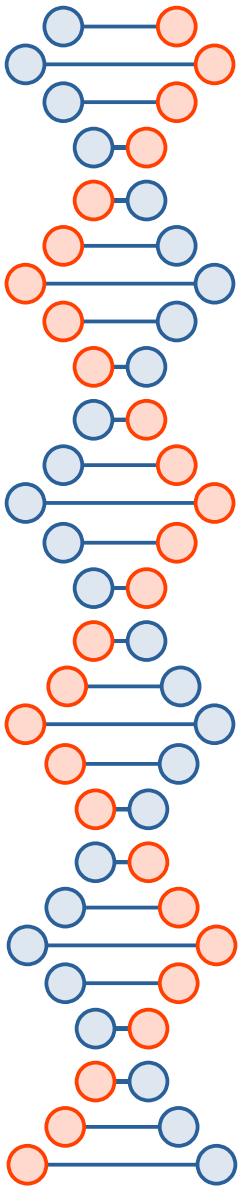
Segurança em Tecnologia da Informação

Msc. Eng. Ali Faiez Taha
Analista de Sistemas – FFCLRP – USP
Departamento de Química
aftaha@usp.br



Segurança em Tecnologia da Informação

- Agenda:
  1) Conceitos
  2) Proteção de dados
  3) Ransomware
  4) Hackers e Crackers
  5) Vulnerabilidades
  6) Servidores e Desktops
  7) Softwares e Ferramentas
  8) Incidentes de Segurança
  9) Recomendações
  10) Segurança da Informação

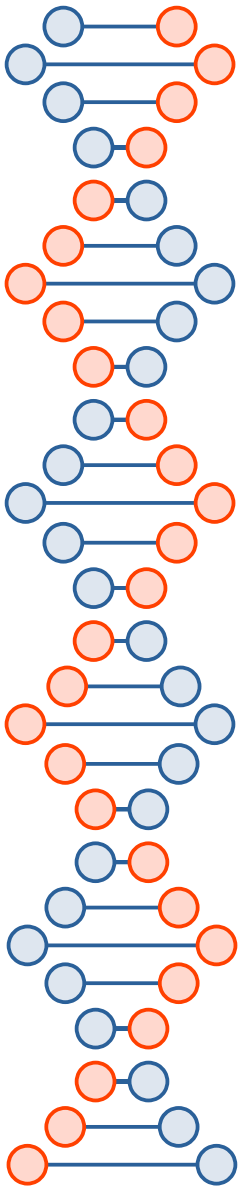


Segurança em TI

- Proteção de um conjunto de dados, preservar o valor dos dados pessoais e/ou de uma organização.
- Prioridades básicas:
  - **Confidencialidade** – protege as informações, forma sigilosa.
  - **Integridade** – informações não sofrem modificações.
  - **Disponibilidade** – disponível ao usuário.
  - **Autenticidade** – fonte confiável.
  - **Irretratabilidade** – impedir que algum usuário negue a autoria da informação, garnatido a autenticidade.
  - **Conformidade** – processos devem obedecer as leis e normas regulamentadas.
  - Norma ISO/IEC 17799:2005, influenciada pelo padrão inglês(British Stantard) BS 7799.
  - http://granito2.rp.usp.br/NBR17799/ https://www.normastecnicas.com/serie-iso-27000/

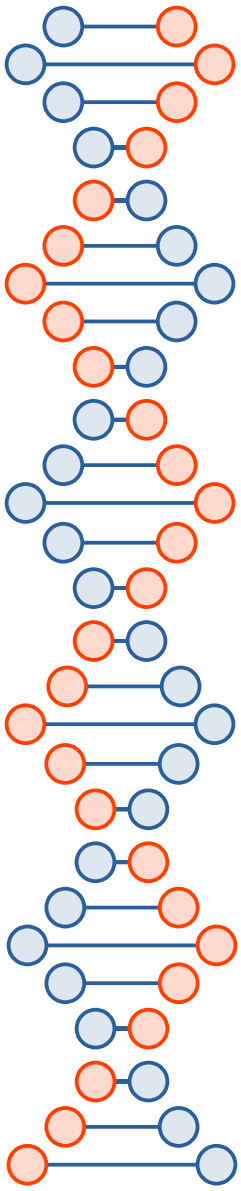
Software e Hardware

- **Servidores:** Dedicados a prover serviços de rede, protocolos de comunicação (TCP/IP), Rede de dados, serviços WEB, Banco de Dados, etc.
- **Desktops:** Computador de uso pessoal com Sistema Operacional e Softwares instalados (Office, programas dedicados, etc).
- **Sistema Operacional:** Windows (Microsoft) , Linux, FreeBSD, Mac OS, etc.
- **Para Segurança em TI**:
- **Software:** Ferramentas de Backup, Softwares Antivírus, Antimalware, Firewall, Proxy, Softwares para controle dos Pais, Recuperação do Sistema, Integridade de memória, Bloqueio dinâmico, Windows Defender (Verificação Antivírus), Criptografia, Verificação de senhas fracas, outros.
- **Hardware**: Firewall – principal aliado na Segurança em TI.



Conexão com a Internet

- **Caiu na Rede, é peixe.**
- **O que é comum acontecer na Rede de Dados:**
- Scans, detecção de Serviços de Rede vulneráveis (www.shodan.io), Descoberta de senhas de Wi-Fi, Servidores com Serviços de rede desatualizados e/ou vulneráveis, Portas TCP/IP abertas, Exploração de falhas em portas TCP/IP, DDOS, ataques de senha (força bruta e dicionário), Injeção SQL, Cross-site scripting (XSS), espionagem, Man in the Middle, Malware, Vírus, Trojans, outros. **https://aiqon.com.br/blog/top-10-os-mais-comuns-ciberataques/**
- **Negação de serviço, Comércio eletrônico, Banco via Internet, Trabalho remoto, vazamento de dados, Privacidade, etc.**
- **Cartilha de Segurança para Internet: https://cartilha.cert.br/**



Monitoração de Software e Hardware

- **Monitoração:** Uso da CPU, Memória, Softwares em execução, tráfego de dados, Discos, Arquivos, SENHAS, Softwares instalados, acesso externo, USUÁRIOS, C*ompartilhamentos*, Periféricos, Pendrives, Sistemas de Backup, Atualização do Sistema Operacional e Softwares instalados.
- **Monitoração da Rede Elétrica**: No-breaks, Moto gerador, Aterramento, Pára-Raios, Tomadas, Ventoinhas, Coolers, Ar Condicionado.
- **Clima:** Raios e trovões, Chuvas, Tempestades, Terremotos, Maremotos, Vendavais, Temperatura e Umidade, extintores de incêndio, etc.
- **Conexões:** WiFi, Bluetooth, Telefone Celular, Rede de dados, Switches, Roteadores, Cabeamento, Impressoras, BACKUP local ou remoto, Equipamentos dedicados, interfaces, etc…

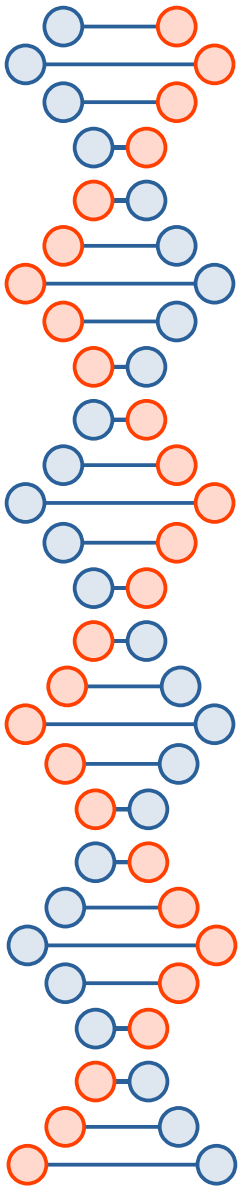
Softwares Maliciosos

- **Softwares Maliciosos (Malwares)**
- ***UM EXEMPLO***
- ***Ransomware:*** *É* um tipo de **malware** que bloqueia o acesso aos dados da vítima.
- Ameaça a publicação ou deleção dos dados até que o resgate seja pago.
- Difícil recuperar os dados. Exigem que se pague o resgate.
- O **Ransomware** criptografa os arquivos da vítimas de uma forma que as torna quase impossível de se recuperar sem uma **chave de descriptografia**.
- Chave de descriptografia fica com quem faz o Ransomware.

kriptos, que significa secreto ou oculto, e graphia, significa escrita.
Criptografia significa escrita secreta

Ransomware

- **Melhores práticas para bloquear o Ransomware:**
- **https://cartilha.cert.br/ransomware/**
- https://www.kaspersky.com/anti-ransomware-tool
- **Não pagar o resgate**
- https://geekflare.com/ransomware-removal-checker-tools/
- https://www.nomoreransom.org/en/index.html
- https://www.nomoreransom.org/en/decryption-tools.html
- **Não pagar o resgate**
- **https://www.controle.net/faq/7-dicas-para-evitar-que-o-ransomware-sequestre-seus-dados**
- **https://www.controle.net/faq/3-softwares-para-remover-ransomware-do-seu-sistema**



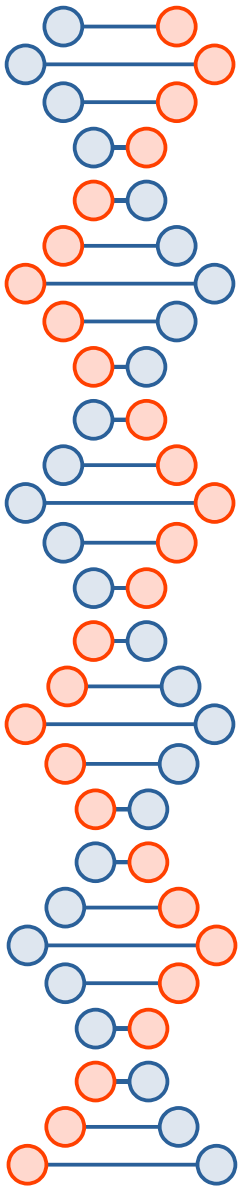
Hacker & Cracker

- **Hacker** é uma palavra da língua inglesa que, no âmbito da informática, designa alguém capaz de invadir dispositivos eletrônicos, redes e sistemas de computação, seja para verificar sua segurança, para aperfeiçoá-lo ou para praticar atos ilícitos.
- **Cracker é um Hacker mal-intencionado.**
- **Hackers** ajudam a identificar falhas de segurança, erros em Softwares, Vulnerabilidades, problemas na Rede de dados, etc.
- São pessoas que se dedicam demais no conhecimento de determinado assunto. Nunca subestime um **Hacker.**
- **Www.significados.com.br/hacker/**
- **Livro : Ética dos Hackers e o espírito da Era da Informação**

Segurança e Hackers

- **O que é necessário para a segurança de TI?**

  Conforme os **hackers** ficam mais experientes, a necessidade de **proteger os ativos digitais e os dispositivos de rede** fica ainda maior.
- Fornecer segurança de TI **é caro.**
- Uma invasão ou violação significativa é **custosa para a empresa**.
- Prejudicam a integridade e podem até fechar uma empresa de pequeno porte.
- * Durante ou após o incidente, a **equipe de segurança de TI** devem obedecer um plano de **resposta a incidentes** como uma ferramenta de **gerenciamento de riscos** para controlar a situação.
- **Qual a diferença entre a segurança de TI e a segurança da informação ?**
- **Segurança de TI** se refere à segurança de dados virtuais, por meio da segurança de rede do computador.
- **Segurança da informação** se refere aos processos e às ferramentas projetados para proteger informações corporativas confidenciais de invasões.



Kevin Mitnick

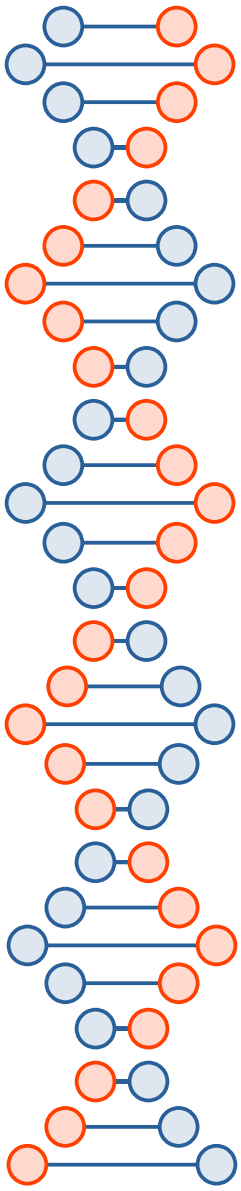
O americano ganhou o título de "hacker mais famoso do mundo" por ser o primeiro conhecido globalmente. A sua vida foi contada em centenas de reportagens e em quatro livros, alguns dos quais adaptados para o cinema. Nascido em Los Angeles em 6 de agosto de 1963, sua paixão por telefonia e sistemas de computador começou aos 13 anos, chegando ao topo da lista dos mais procurados do FBI. No entanto, suas habilidades de hacker permitiram que ele escapasse da captura pelas autoridades por muitos anos. Em 1993, ele conseguiu controlar os sistemas telefônicos da Califórnia, algo que lhe permitiu também grampear os telefones dos agentes que o procuravam e enganá-los.

No final, outro especialista em segurança cibernética o pegou, o japonês Tsutomu Shimomura, que havia se tornado rival de Mitnick após um duelo bizarro na rede. Tudo começou no dia de Natal de 1994, quando o americano roubou e-mails do hacker japonês e zombou dele. Ao saber do ataque, Shimomura se ofereceu para ajudar o FBI a rastrear Mitnick. Usando um software capaz de reconstruir sessões no computador de um usuário, Shimomura conseguiu rastrear o pai de todos os hackers alguns meses depois, levando à sua captura em fevereiro de 1995.

Ele foi condenado a cinco anos de prisão por obter acesso a cerca de 20.000 números de cartão de crédito, incluindo alguns pertencentes a magnatas do Vale do Silício, por meio de suas habilidades de hacker. Na verdade, nenhuma evidência foi encontrada de que Mitnick usou os arquivos que roubou para enriquecer. Ele mesmo se defendeu dizendo que suas atividades nada mais eram do que "uma forma de jogo de alto risco", mas não prejudicou ninguém.

Kevin Mitnick

- Sua captura causou grande agitação no mundo dos hackers de computador, onde Mitnick era considerado mais uma lenda do que um homem. Em 1998, enquanto aguardava a sentença, um grupo de apoiadores conseguiu invadir o site do The Times , obrigando o jornal inglês a fechar por várias horas. Além disso, foi criado um movimento mundial de apoio conhecido como "Free Kevin", pedindo a libertação do hacker ou pelo menos a revisão da sentença, considerada dura demais com relação aos crimes cometidos.
- Por fim, Mitnick chegou a um acordo judicial e, após se declarar culpado de fraude eletrônica e de computador, foi libertado da prisão em 2000, embora em estado grave. Por três anos ele foi proibido de se aproximar de um computador ou celular sem a permissão de seu oficial de condicional, pois, segundo o promotor, com apenas uma ligação ele era capaz de causar um holocausto nuclear. Após sair da prisão, o hacker voltou a insistir na falta de má-fé em suas ações: “Meus crimes foram simples crimes de invasão de propriedade. Meu caso é um caso de curiosidade”.
- Quando conseguiu se reconectar à rede, Mitnick decidiu se tornar um hacker "do bem", usando suas habilidades a serviço de empresas ou instituições governamentais. Ele fundou a empresa KnowBe4, que se descreve como “a provedora do maior treinamento de conscientização de segurança do mundo”. Em seu site, a empresa diz que aconselha mais de 60.000 organizações que usam o currículo de treinamento em segurança cibernética que Mitnick projetou.
- https://www.youtube.com/watch?app=desktop&v=ZJPfL-mwLks



Os cinco maiores hackers do mundo

1 - Pranav Hivarekar

Em 2016, Pranav Hivarekar, um dos maiores hackers do mundo, ganhou uma recompensa de cinco dígitos em dólares ao descobrir uma falha do Facebook.

Algum tempo antes de ser recompensado, mais especificamente, 8 horas, a rede social havia anunciado que as pessoas poderiam comentar em postagens usando vídeos. Foi assim que o hacker começou sua investigação. Após analisar todo o código e buscar bugs, ele descobriu que, com o comando certo, poderia apagar qualquer publicação. Até mesmo uma postagem do próprio Mark Zuckemberg.

Os cinco maiores hackers do mundo

2 - David L. Smith

Seria a história de David L. Smith uma história de redenção? Em 1999, o programador desenvolveu um vírus chamado worm Melissa que tirou vários provedores de e-mail do ar. Foram milhares de empresa prejudicas, resultando em um impacto financeiro de mais de US$80 milhões.

Condenado a prisão por 10 anos, em 2002, ele recebeu uma proposta do FBI para reduzir sua pena: proteger novos sistemas, encontrar vulnerabilidades e identificar futuros invasores.

Os cinco maiores hackers do mundo

3 - Kevin Mitnick

De um dos maiores hackers da história à palestrante sobre cyber segurança, a trajetória de Kevin Mitnick esbarra em alguns pontos com a de David L. Smith. Em 1979, ele se tornou uma referência na área ao acessar ilegalmente a rede da Digital Equipment Corporation. Na época, a empresa foi uma das pioneiras no desenvolvimento dos computadores.

Além de vazar senhas, ele também visualizou e-mails confidenciais e roubou um software. Acusado de crime virtual, uma caçada foi iniciada contra Kevin Mitnick, considerado o maior criminoso virtual de todos os tempos. Enquanto ele fugia, conseguiu, também, vazar dados e segredos de duas gigantes da época: Nokia e Motorola.

Alguns anos depois, após ser preso e cumprir sua pena, ele se tornou consultor em segurança, palestrante e dono de uma empresa voltada para **hacker ético**.

Os cinco maiores hackers do mundo

4 - Shivam Vashisht

- Encontrar bugs se tornou uma profissão, ainda mais para jovens de 18 a 29 anos. Em 2019, Shivam Vashisht ganhou mais de US$125 mil somente fazendo isso. Em parceria com uma hacker norte-americana, Jesse Kinser, eles transformaram o hobby em uma profissão.
- E o melhor, não é preciso ter grandes qualificações e/ou títulos para ser bom na área. Basta, apenas, conhecer a fundo os sistemas e entender de hacker ético.

Os cinco maiores hackers do mundo

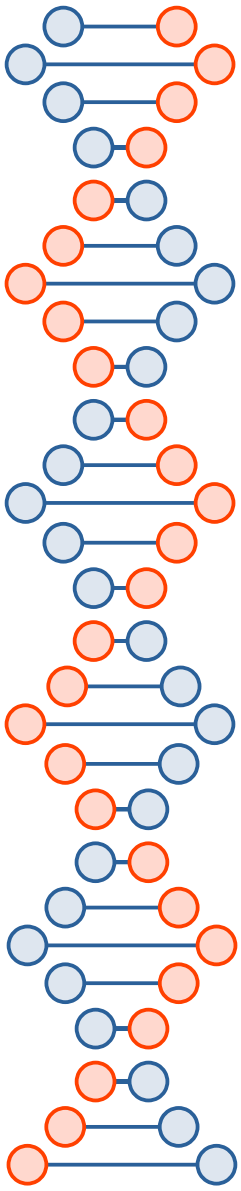
5 - Kevin Poulsen

Antes de ser um jornalista prestigiado do New York Times, Kevin Poulsen era chamado de “Dark Dante”, hacker conhecido por invadir sistemas telefônicos. No entanto, não pense que sua atuação para por aí. Um de seus atos mais notórios foi quando ele invadiu uma estação de rádio e alterou os vencedores de uma competição.

Competição a qual, quem vencesse, seria presenteado com um Porsche. Por outro lado, para o FBI, seus maiores crimes foram relacionados a invasão de telefonias. Tanto que foi o que rendeu sua prisão alguns anos após.

Condenado a 51 meses, além de ter que pagar uma multa de US$56 mil, ao sair da cadeia, a vida de Kevin tomou outros rumos. O primeiro passo foi criar um software que facilitava a relação entre jornalistas e fontes, Secure Drop. O segundo, ele começou a atuar como editor e colaborador de vários jornais prestigiados.

- https://www.youtube.com/watch?v=-wbF7r_sGHk



Os 5 Maiores Hackers Do Brasil

1 - Daniel Lotrano Nascimento, como é mais conhecido, se tornou um dos maiores hackers do Brasil antes mesmo de completar 18 anos. Entre os 11 e os 15 anos de idade, o jovem invadiu servidores brasileiros e estrangeiros. Outro de seus feitos que chamam atenção foi quando atacou a Telemar, atual Oi.

A consequência de seus atos fez com que uma parte do nosso país ficasse sem internet por uma semana.

Após ser preso e pagar pelo que fez, ele mudou de área. Em 2017, lançou um livro com repercussão midiática onde contou parte da sua história como ex-hacker. O impacto disso fez com que ele pudesse montar a sua própria elite de hackers, que presta serviço para projetos sociais, governo, empresários e muito mais.

2 - Wanderley de Abreu Júnior, ou só Storm, ficou conhecido por invadir o sistema da NASA aos 17 anos. Aos 20, participou de uma iniciativa para identificar pedófilos online e encontrou mais de 200 nomes. Um dos maiores hackers do Brasil ele um pouco após, trabalhou em um sistema de navegação espacial e em outro relacionado a criptomoedas.

Já na pandemia, criou o Mercado Gaia, que auxiliou no escoamento da safra de alimentos e serviu de apoio para várias comunidades carentes durante a crise. Fato é, hoje, Storm, é uma das referências da área. Não só pelo que fez enquanto cracker, quanto pelo que se propôs a fazer sendo um hacker ético.

Nos dias atuais, além de empresário, ele também presta serviço como consultor digital.

Os 5 Maiores Hackers Do Brasil

3 - Marco Aurélio Thompson

Além de ser considerado um hacker brilhante, em 2003, Marco Aurélio Thompson criou um curso para ensinar pessoas a como invadir um sistema. Professor, escritor, jornalista e hacker ético, foram mais de 37.000 alunos formados em todo o país. Também é conhecido como um dos maiores hackers do Brasil ele é

Com 3 bacharéis e 5 licenciaturas, ele é, sem sombra de dúvidas, considerado como um dos nomes mais brilhantes do Brasil. Se você tem interesse na área, vale a pena conhecer um pouco mais da sua trajetória e, até mesmo, comprar um de seus cursos ou livros.

4 - Vinícius Camacho

Embora não tão popular quanto os outros nomes da lista, Vinícius Camacho (K-Max) é conhecido na mídia como o “hacker que irritou as telefonias”. Parte disso por ter descoberto uma falha nas empresas e, para comprovar sua teoria e mostrar o quão grave era, ter divulgado, parcialmente, alguns dados pessoais de clientes.

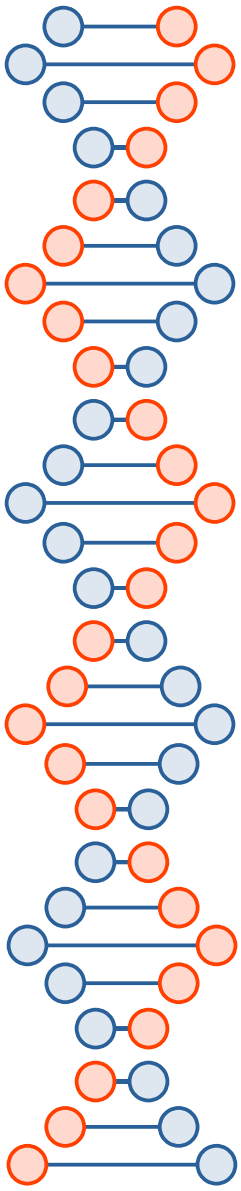
Outro fato que chamou atenção foi quando, em 2005, roubou comunidades no Orkut. Em uma entrevista para a revista Época, novamente, ele revela que o seu objetivo era somente ajudar e mostrar as vulnerabilidades dos sistemas.

Em 2009 ele foi indiciado, sendo que, atualmente, presta serviço como Analista de Cyber Segurança na MIDRI. Assim como outros nomes da lista, hoje em dia, ele atua como hacker ético para empresas.

5 - Rodrigo Rubira Branco

Rodrigo Rubira Branco ou só BSDaemon é um nome visto com muito carinho na comunidade hacker. Palestrante, diretor de pesquisa e desenvolvimento e, atualmente, engenheiro na Amazon, foi um dos primeiros a discutir sobre malwares e vulnerabilidade no Brasil.

Reconhecido, também, internacionalmente, ele possui um longo currículo e é uma das referências da área.



O maiores ataques hackers

1 – Yahoo

O ataque aconteceu em 2013 e comprometeu 3 bilhões de contas. Dados como nomes, endereços de e-mail e senhas foram vazados, a situação se repetiu em 2014, e 500 milhões de contas foram afetados.

2 – Sony

Em 2011, a empresa sofreu um ataque que aconteceu através de DDoS, em seguida aconteceu o vazamento de dados de 77 milhões de usuários do Playstation Network.

Já em 2014, 100 terabytes de dados foram invadidos, contendo informações como dados de funcionário, filmes e etc.

3 – Ebay

Em 2014, a empresa sofreu um ataque que comprometeu dados de 140 milhões de contas.

Os hackers tiveram acesso a endereços de e-mail e senhas criptografadas dos usuários da plataforma.

O maiores ataques hackers

4 – Comitê Nacional Democrata

Em 2016, o Partido Democrata americano sofreu um ataque hacker que foi responsável pelo rouvo de 20 mil e-mails e 8 mil anexos de informações sigilosas sobre os membros do alto escalão do partido.

O ataque teve um impacto significativo nas eleições americanas.

5 – Equifax

A empresa de gestão de crédito americana, sofreu um ataque hacker em 2017 que comprometeu cerca de 143 milhões de dados de clientes.

As informações confidenciais como nome, data de nascimento, números da previdência social e carteira de habilitação foram vazadas.

Principais ameaças virtuais

Vírus

O vírus é um **software**, geralmente malicioso, que atua se replicando e infectando arquivos e programas de computadores. Desse modo, quando esses arquivos são executados, ele é ativado e espalhado, podendo comprometer de maneira muito grave os sistemas computacionais, causando lentidão através do consumo de recursos, corrompendo arquivos, roubando informações, danificando softwares, entre outras consequências.

Esse malware se anexa a um arquivo ou programa, permanecendo inativo. Quando o arquivo é executado, o vírus é ativado, infectando todo o sistema. Desse modo, é possível que um vírus fique inativado em um computador por muito tempo, sem causar nenhum problema, até ser executado por alguma ação externa.

FIQUE ATENTO: O vírus sempre precisará de um hospedeiro, como um documento de arquivo, para poder se acomodar e se replicar. **Eles não são auto suficientes.**

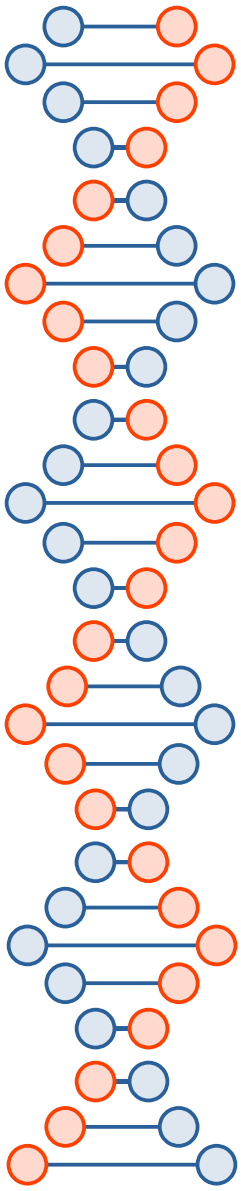
A propagação de um vírus pode acontecer de diversas maneiras, através de anexos de e-mail, downloads de arquivos da internet, links, pen drives, entre outros meios.

O vírus possui três partes:

Mecanismo de Infecção: São os meios ou formas pelas quais um vírus se propaga, habilitando-o a se reproduzir. Ou seja, é COMO ele se propaga.

Mecanismo de Ativação: É a condição/evento que determina quando o vírus será ativado, ou seja, é QUANDO a carga útil é ativada ou entregue.

Carga útil: A carga útil é o seu EFEITO, ou seja, os danos que ele pode causar.

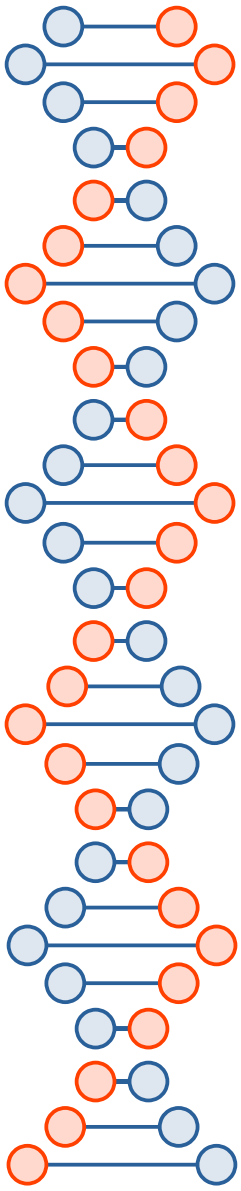


Trojan Horse

Cavalo de Tróia

Também conhecido como **Trojan Horse**, o Cavalo de Tróia é um malware que infecta um computador disfarçado de um **software** legítimo.

Ao mesmo tempo que ele se passa por um programa que simula alguma funcionalidade útil para o usuário, ele esconde um **software** malicioso que pode trazer prejuízos ao computador.



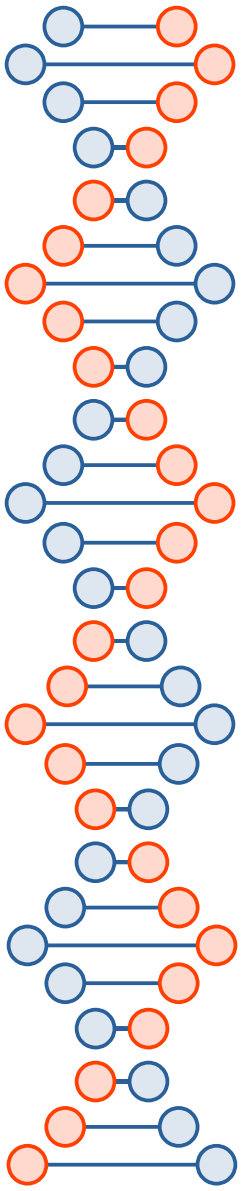
Worm

O Worm, diferentemente do vírus, é um programa independente e que possui a característica de se autorreplicar em sistemas informatizados, sem a necessidade de utilizar um programa hospedeiro.

Ele possui a capacidade de causar danos sem a necessidade de ser ativado pela execução do usuário. A sua atuação engloba a exploração de falhas e vulnerabilidades de sistemas de informação, podendo ocasionar graves danos à sua funcionalidade, além da possibilidade de realizar o roubo de informações, entre outros danos.

WORM ➜ Não precisa de hospedeiro / Não precisa ser ativado por meio de alguma execução.

VÍRUS ➜ Precisa de hospedeiro / Precisa ser ativado por meio de alguma execução.



Bots

Bot

O **bot**, também chamado de **robô**, é um código malicioso que infecta computadores e permite que um criminoso possa controlá-los remotamente, sem o conhecimento do dono da máquina. Dessa maneira, ao ser realizada essa comunicação, o invasor pode enviar instruções maliciosas para serem executadas no computador, podendo roubar informações, além da possibilidade de causar sérios danos ao seu funcionamento.

A sua maneira de propagação é similar ao worm, replicando-se automaticamente, sem a necessidade de um hospedeiro.

O Botnet é uma rede de computadores infectados, com o intuito de potencializar as atividades danosas dos bots.

Spyware

Spyware

Spyware, ou Software Espião, é um tipo de malware cuja função é se infiltrar em sistemas computacionais, com o intuito de coletar informações pessoais ou confidenciais do usuário, sem o seu conhecimento, e as enviar ao invasor remotamente pela internet.

Dois tipos de Spywares são o keylogger e o screenlogger.

Keylogger: esse tipo de spyware é capaz de coletar, armazenar e enviar a criminosos todas as informações que são digitadas no teclado pelo usuário, como sites visitados, senhas, entre outras informações.

Screenlogger: é um tipo de spyware que tira prints (fotos) da tela do computador, informando onde o cursor do mouse é clicado, repassando informações sigilosas do usuário, como senhas, entre outros danos. Ele funciona de maneira similar ao keylogger, mas em vez de gravar as teclas digitadas, ele grava a tela do usuário.

Adware

Adware

Esse **malware**, cujo nome é derivado da expressão **“Advertising Software“**, é projetado para mostrar anúncios de sites e produtos na tela do usuário, geralmente de maneira indesejada. Apesar desse programa não ser um tipo de malware muito perigoso, ele pode gerar bastante incômodo às pessoas que utilizam a internet.

Alguns deles são considerados um tipo de **Spyware**, pois os hábitos dos usuários durante sua navegação na internet são monitorados, permitindo que sejam exibidas propagandas de produtos relacionados às suas pesquisas. Você já deve ter percebido que quando você realiza uma pesquisa de algum produto na internet, todas as suas redes sociais são inundadas com propagandas de diversos lugares a respeito deste produto. Isso se deve à ação dos **adwares**.

Backdoor

Backdoor

O Backdoor, código malicioso conhecido também como **Porta dos Fundos**, ao infectar um computador, cria falhas nos sistemas de segurança do sistema, permitindo que outras ameaças virtuais invadam o sistema.

A sua atuação é focada na abertura das portas dos fundos do sistema computacional, permitindo que malware e invasores ingressem no sistema operacional da máquina, sem o conhecimento do usuário.

Ransomware

Ransomware

Essa ameaça virtual é capaz de sequestrar os documentos, arquivos e informações de um usuário, **tornando-os inacessíveis**, geralmente mediante **criptografia**, e apenas os liberando através de pagamento (**ransom**) da vítima. Além disso, ele também é capaz de impedir o acesso do proprietário ao seu equipamento infectado.

Uma maneira de amenizar os prejuízos causados por esse **malware é realizar um backup regular dos seus arquivos**, de modo que, caso um invasor os sequestre, haverá uma cópia desses documentos.

Rootkit

Rootkit

Esse código malicioso não possui o objetivo de causar danos diretos ao computador, ele apenas assegura que **outros códigos invasores não sejam descobertos pelo sistema e pelo usuário**. Caso um computador seja infectado por um **malware** que possa ser nocivo ao seu funcionamento, o **rootkit** atua de modo a **esconder os vestígios da atuação dessa ameaça virtual, deletando os indícios dessa invasão.**

Em outras palavras, o **rootkit não atua para obter dados e acesso privilegiado ao sistema, mas para garantir que outros malwares continuem atuando sem serem descobertos.**

- **Conheça as ferramentas CHKROOTKIT e RKHUNTER, para detectar Rootkits.**

Hijacker

Hijacker

Você já instalou um **software** novo no computador e, de repente, você percebe que sua ferramenta de pesquisa no seu navegador foi alterada para outro site, ou nota a presença de novas barras de ferramentas ao acessar à internet?

Pois bem, quando isso acontece, provavelmente é porque seu computador foi infectado por um Hijacker.

Esse **malware** atua nos navegadores de internet do computador, alterando a página inicial do usuário, abrindo **pop-ups** indesejados, instalando barras de ferramentas, extensões, mudando a ferramenta de pesquisa, forçando a abertura de outras páginas que não são desejadas pelo usuário, podendo até impedir o acesso de alguns sites, como as páginas de antivírus.

Malwares

- **EMOTET – O Malware mais perigoso do mundo**

  Você já ouviu falar em “emotet”? Ao contrário do que muitos pensam, não se trata de um vírus. Ele apareceu pela primeira vez como um trojan bancário em 2014, visando interceptar dados de acesso online de clientes bancários alemães e austríacos.

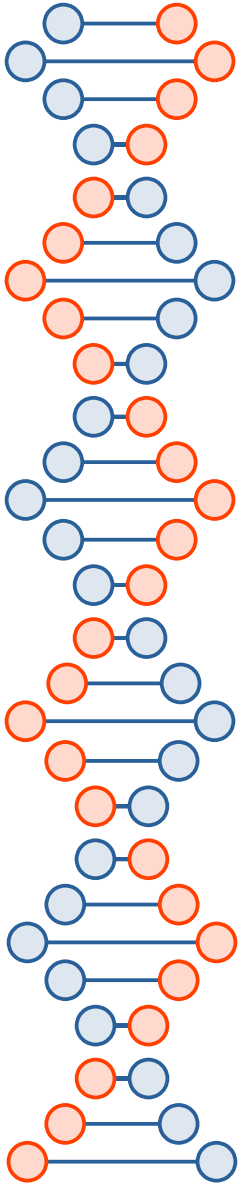
  No entanto, o emotet também pode carregar e executar um grande número de módulos com outras funções maliciosas. Apesar de ser originalmente projetado como um malware bancário, capaz de roubar informações confidenciais, suas versões posteriores se tornaram cada vez mais devastadoras, com funcionalidades que o ajudam a evitar a detecção por algumas soluções de segurança antimalware.

- Atualmente, o emotet usa vários truques para tentar impedir a sua identificação e a análise. Ele sabe se está sendo executado dentro de uma máquina virtual (VM) e ficará inativo se detectar um ambiente de sandbox, que é uma ferramenta que os pesquisadores de segurança cibernética usam para observar malwares em um espaço seguro e controlado.

- https://www.psafe.com/blog/conheca-o-emotet-ou-o-malware-mais-perigoso-do-mundo/

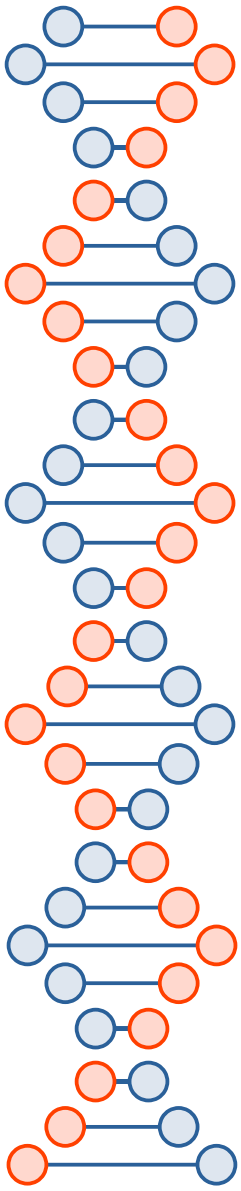
Segurança na Internet

- Internetsegura.br
- Para todos
- **Cuidados e responsabilidades no uso da Internet.**
- **Internet segura para seus filhos.**
- **Internet segura com responsa na sala de aula.**



Incidentes de Segurança

- Quando ocorrer incidente, basta comunicar via E-Mail.
- **Na USP: https://security.usp.br**
- Para comunicar um Incidente, basta enviar E-Mail (para security@usp.br) com os **arquivos de log** coletados e todos os dados sobre o problema ocorrido.
- **Exemplo:** Máquina infectada com vírus tentando atacar outras máquinas pelo mundo.
- A **STI da sua Unidade-USP** será notificada e o incidente será examinado e solucionado.
- Estatísticas mantidas pelo CERT.BR: **https://stats.cert.br/**

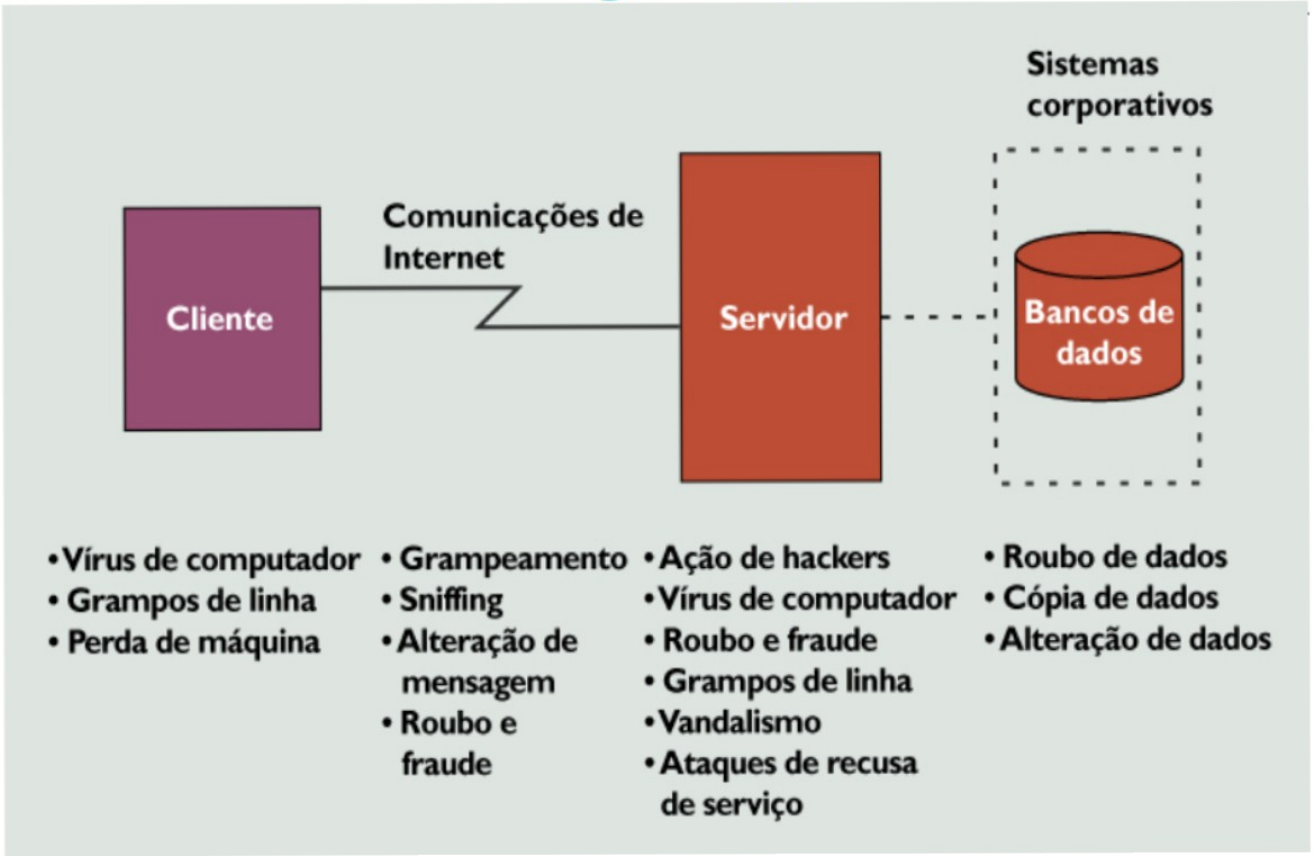


Segurança da Informação

- **A Tecnologia da informação:** ferramenta capaz de alavancar os negócios quando seu uso está vinculado à medidas de proteção dos dados Corporativos.
- **Modelo de Segurança da Informação**: investimento capaz de assegurar a sobrevivência da Empresa e a continuidade dos negócios da Organização.
- Empresas competitivas devem contar com um trabalho de **profissionais especializados e qualificados** que saibam como alinhar Segurança a Tecnologia da Informação.

Segurança na Internet

Desafios de Segurança na Internet



Ciberataques

1 – Denial-of-Service (DoS) e o distributed denial-of-service (DDoS)

2 – O ataque Man-in-the-middle (MitM)

3 – Ataques de phishing e spear phishing

4 – Ataques de Drive-by

5 – Ataques de senha

6 – Ataque de injeção SQL

7 – Ataque de Cross-site scripting (XSS)

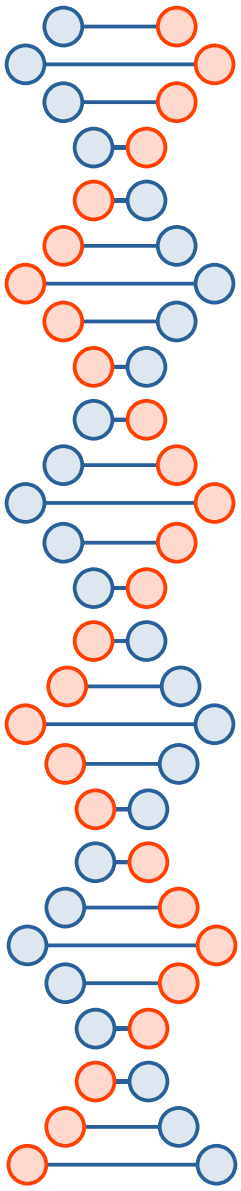
8 – Ataque de espionagem

9 – Ataque de aniversário

10 – Ataques de Malware

https://aiqon.com.br/blog/top-10-os-mais-comuns-ciberataques

- Mantenha seus sistemas e banco de dados de vírus atualizados, treine seus funcionários e configure o seu firewall para permitir a entrada apenas de portas e hots específicos que você precisa, mantenha suas senhas fortes e use o modelo de privilégio mínimo no seu ambiente de TI, faça backups regulares e audite continuamente seus sistemas de TI para atividade suspeita.



Prioridades

Por que priorizar a segurança da informação

Em 2017 empresas de todo mundo foram vítimas de **ramsonwares** que desestabilizaram o seu ambiente. E ainda continua…

Os ataques dos vírus WannaCry e Bad Rabbit ganharam as manchetes do jornal e assustaram usuários e profissionais de TI.

A segurança da informação deve ser sempre colocada entre as prioridades na sua área de TI

A informação é o bem mais valioso de uma empresa. Desta forma, a sua exposição pode levar uma organização a falência, dependendo do caso.

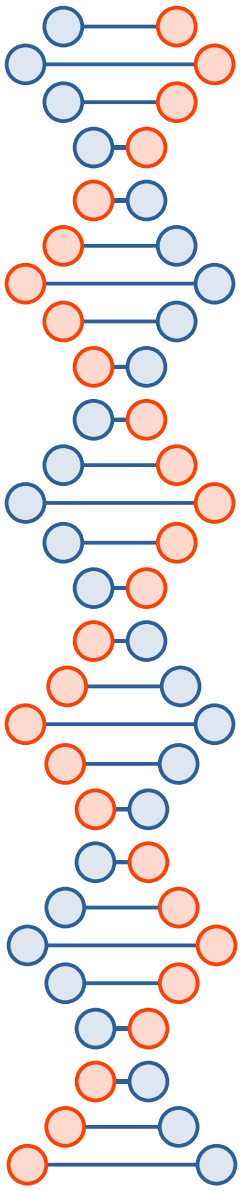
A perda de credibilidade e de vantagem competitiva são algumas das consequências do vazamento de informações para uma empresa.

O **investimento** em segurança da informação proporciona a confiança, que é tão essencial na manutenção de uma boa relação comercial.

Treinamento da equipe de Tecnologia da Informação.

RFC 2196
Site Security Handbook

- Este manual é um guia para desenvolvimento de políticas de segurança de computador e procedimentos para sites que têm seus sistemas na Internet.
- O propósito deste manual é proporcionar um guia prático aos administradores tentando tornar segura uma grande variedade de informações e serviços.
- Os assuntos abordados incluem os conteúdos de política e formação, tópicos técnicos de segurança de redes, e, também, reações a incidentes de segurança.
- **http://penta.ufrgs.br/gereseg/rfc2196/**



Gestão da Segurança da Informação

- Palestra apresentada no GEINFO 10, em 2011
- http://granito2.rp.usp.br/SGTI/Gestao.Seg.Informacao.Ali.Faiez.Taha.Geinfo2011.pdf

  A Gestão da Segurança da Informação visa a adoção de medidas alinhadas com as estratégias de negócio, a partir de um monitoramento contínuo dos processos, métodos e ações.
- Tem por objetivo o pronto restabelecimento dos sistemas, evitar acesso indevido à informações, mitigar sistemas, mitigar os riscos e se basear nos 3 pilares da GTSI:
- **Confidencialidade , Integridade e Disponibilidade**

Prioridades

As atividades da área de segurança da informação

As atribuições dos profissionais de segurança da informação envolvem muitos fatores.

Instalação e configuração das soluções de segurança, tais como: antivírus, firewall, antimalware, antispyware, antiramsonware e etc.

Tudo isso a fim de filtrar os conteúdos que serão executados nas estações de trabalho, protegendo as informações contra roubo, alterações e destruição.

Constante monitoramento das redes de dados, a fim de evitar ou minimizar os danos causados por ataques.

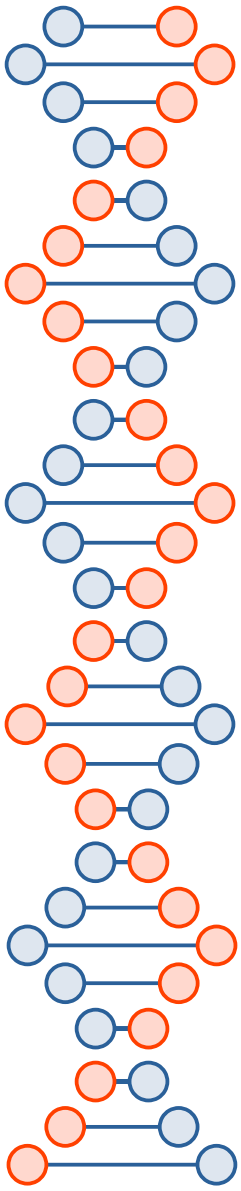
Atentar às falhas em sistemas de terceiros, que venham a serem descobertas.

Atenta às falhas divulgadas nos meios competentes. Aplicar as correções fornecidas pelos desenvolvedores dos sistemas.

Estabelecer políticas e normas, que devem ser seguidas pelos usuários, a fim de garantir o bom uso dos recursos da organização.

Definição das políticas de acesso aos dados, de acordo com o nível hierárquico ou por departamento.

Bloqueio de sites, sistemas e softwares considerados perigosos ou não estejam de acordo com as políticas definidas pela área.



Casos e mais casos...

Apagão - Prejuízos, custos, Backup/Energia

Incêndios-Tipos, causas e prejuízos

Vazamento de informações - criptografar ?

Hackerismo – crimes computacionais

Violação do Direito Autoral – prejuízo comercial e reputação

Espionagem - monitoração

Falhas em Sistemas – qualidade de produtos

Ataques a servidores – proteger mais

Resposta a incidentes - Conscientização

Roubo de senhas e de dinheiro (mercado hacker) - Botnets

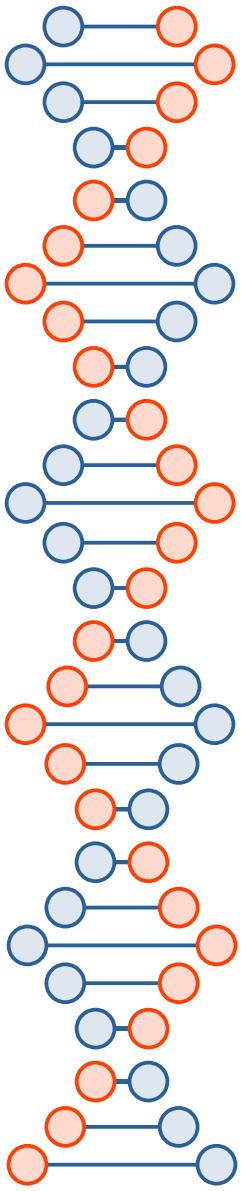
Nível de dependência de externos, de fornecedores de serviços – custo de hora parada

Fraudes e seus impactos - $financeiro$, reputação

outros …

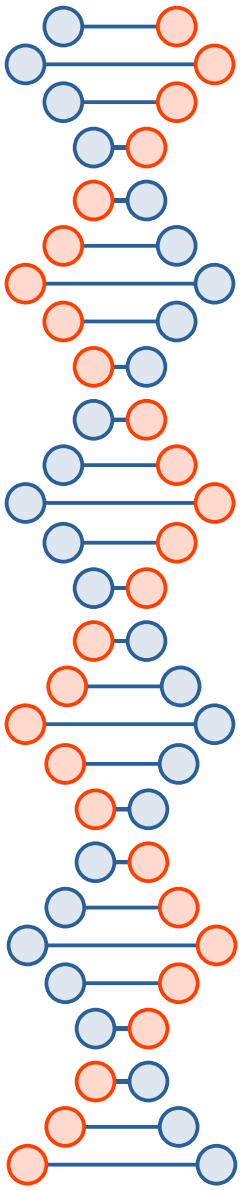
Programas importantes

- Programa de Privacidade e Segurança da Informação (www.gov.br)
- Centro Integrado de Segurança Cibernética (CISC Gov.br)
- Lei de Acesso à Informação (www.gov.br)
- Marco Civil da Internet
- Lei Geral de Proteção de dados
- Seminário de Proteção à Privacidade e aos Dados Pessoais
- Comissão Especial de Direito Digital da Câmara dos Deputados
- Projeto Cidadão na Rede (cidadaonarede.nic.br)
- Segurança da Informação e Segurança Cibernética – (sites.tcu.gov.br)
- Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber) (Gabinete de Segurança Institucional da Presidência da República Secretaria de Segurança da Informação e Cibernética)
- Defesa e segurança cibernética dos serviços públicos – Senado Federal
- Glossário Segurança da Informação
- Privacidade Digital (www.privacidade.digital/)
- Vigilância e Espionagem Digital
- Dia Nacional da Proteção de Dados – Senado Federal
- Regulação da Inteligência Artificial no Brasil – Senado Federal
- Política Nacional de Educação Digital – Senado Federal



Perguntas ?

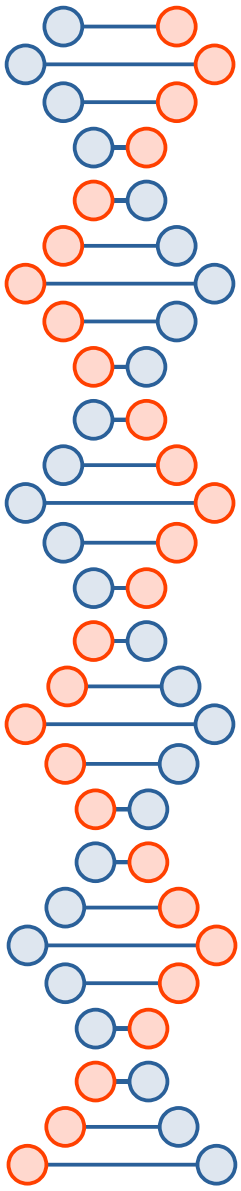
Perguntas ?



Política Segurança de Informação

Política de Segurança da Informação

- Definição dos agentes envolvidos em segurança da informação dentro das Empresas
- Classificação de Informações
- Política de acessos externos
- Política de acesso interno
- Política de uso da Intranet
- Política de uso da Internet
- Eventos mínimos a serem logados nos Sistemas Corporativos
- Trilhas de auditoria
- Política de Backup
- Política de uso de software
- Acesso físico
- Acesso Lógico



USUÁRIOS

Projeto de Conscientização de Usuários

- Segurança Física
- Segurança Lógica
  - Backup
  - Pirataria
  - Vírus
  - Intranet e Internet
  - Plano de Contingência
  - Classificação da Informação
  - Auto-Treinamento de Segurança Tecnológica

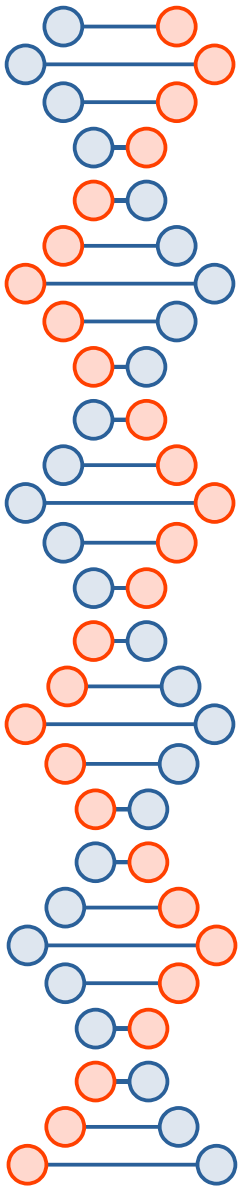
Plano de Contingência

Plano de Contingência

- Análise de riscos do ambiente computacional
- Definição da criticidade dos Sistemas Corporativos
- Definição da criticidade dos módulos críticos dentro dos Sistemas considerados críticos
- Definição da Infra-estrutura básica para processamento em caso de contingência.
- Definição dos recursos de Software e Hardware necessários para processamento dos Sistemas
- Definição das equipes de contingência
- Plano de retorno

Backup Site

- Cold-Site próprio
- Cold-Site de Terceiros
- Hot-Site próprio
- Hot-Site de terceiros
- Hot-Site próprio compartilhado



Backup, Intranet e Internet

Backup de Dados

- Periodicidade de Backup
- Definição de tecnologica e mídia a serem adotadas
- Sala-cofre
- Alternativas de Backup externo
- Ferramentas de gerenciamento de Backup

Gerenciamento e Segurança em Intranets

- Ferramentas de Gerenciamento de Intranet
- Criptografia
- Anti-Vírus
- Anti-Trojans

Gerenciamento e Segurança na Internet

- Ferramentas de Gerenciamento da Internet
- Criptografia
- Anti-Vírus
- Firewall
- Proxy
- Filtros
- Certificação
- Formas de endereçamento do domínio interno

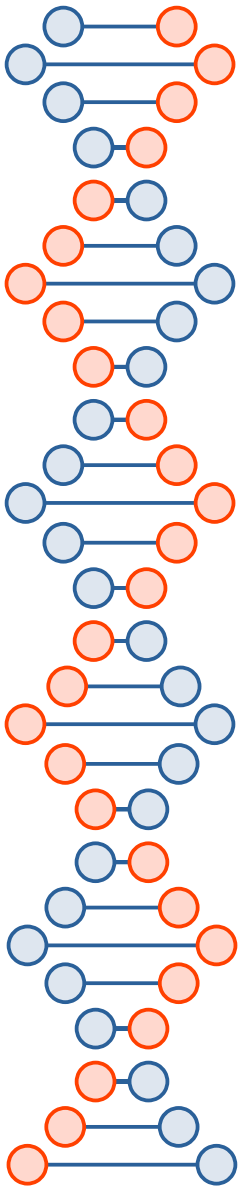
Segurança Física e Lógica

Projeto de Segurança Física

- Condições Ambientais
- Definição de áreas críticas
- Sala de Monitoração
- Pontos para uso de câmeras
- Portas eclusas
- Treinamento especializado para a vigilância patrimonial em ambientes de processamento de dados

Projeto de Segurança Lógica

- Monitoração de cadastramento
- Log de eventos críticos
- Log dos sistemas de segurança
- Trilhas de auditoria
- Metodologia de Desenvolvimento de Sistemas



Controles

- Adotar controles físicos, tecnológicos e humanos personalizados que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio.
- Referências:

https://edisciplinas.usp.br/pluginfile.php/3530720/mod_resource/content/0/Aula09-Seguranca-Controle-SI.pdf

- **https://www.iso27001security.com/** **https://www.normastecnicas.com/serie-iso-27000/**
- **Portal GEDWEB: https://www.gedweb.com.br/** ***Usar Senha Única da USP***