# CISEF


# Segurança Cibernética

## Uma Questão de Sobrevivência

Um guia preparatório para certificação EXIN Cyber & IT Security Foundation

academy

CISEF


# Segurança Cibernética

## Uma Questão de Sobrevivência

Um guia preparatório para certificação EXIN Cyber & IT Security Foundation


academy

"Este conteúdo foi preparado pela PMG Academy (parceiro oficial) e segue os guidelines do EXIN, auxiliando o profissional na preparação para o exame EXIN Cyber & IT Security Foundation.
O EXIN não se responsabiliza pelo conteúdo e/ou qualquer ideia que venha a ser expressada pelo autor, sendo o mesmo responsável pela obra". (EXIN)

ISBN nº 978-65-995022-0-0

Copyright © 2021 PMG Academy
Todos os direitos reservados

# CISEF

Segurança Cibernética – Uma Questão de Sobrevivência

Produção da PMG Academy.
Brasil/SP/2021_ Edição 01

Este livro é um guia preparatório para certificação EXIN Cyber & IT Security Foundation

# Conteúdo

# Apresentação

Este livro é mais que um guia preparatório para certificação EXIN Cyber & IT Security Foundation; é um conteúdo que pode também ser aproveitado para enriquecer seu conhecimento e somar capacitação à sua bagagem profissional.
Trata-se de uma abordagem sobre os fundamentos da Segurança Cibernética, identificando na infraestrutura básica dos sistemas de informação e em sua funcionalidade, os cenários de vulnerabilidades, ameaças, riscos e as devidas estratégias de mitigação relacionadas.

# Sobre a certificação EXIN

O EXIN Cyber & IT Security Foundation é um certificado de excelência em Programação Segura! É o diferencial para quem é visionário e sabe que precisa se qualificar no mercado para atender essa demanda, pois aborda justamente tópicos relacionados à segurança cibernética, como:

- Sistemas de computador;
- Aplicações e bancos de dados;
- Redes TCP/IP;
- Criptografia;
- Gerenciamento de identidade e acesso;
- Computação em nuvem;
- Exploração de vulnerabilidades.

Por isso, este livro é a oportunidade perfeita para você se preparar e conquistar o certificado EXIN Cyber & IT Security Foundation e dar esse upgrade na sua vida profissional!

Lembrando que a certificação EXIN Cyber & IT Security Foundation testa candidatos no Bloom Nível 1 e Nível 2, seguindo a Taxonomia de Bloom Revisada, que é um instrumento de estudo que identifica o nível de desenvolvimento cognitivo educacional do indivíduo. Dessa forma, podemos definir:

O BLOOM NÍVEL 1 como "remembering", que quer dizer "lembrança", e se refere à recuperação de informações. Ou seja, os candidatos precisam absorver, lembrar, reconhecer e recordar. Para quem está neste nível, a lembrança é o elemento foco na aprendizagem para que se possa avançar para os níveis mais elevados.

BLOOM NÍVEL 2, que se refere à "compreensão", "understanding". Considerado um nível acima da "lembrança". O "entendimento" aqui, no nível dois, mostra que é possível os candidatos compreenderem o conteúdo e avaliarem como utilizar o material de aprendizagem em seus próprios ambientes.

# Introdução

Cada vez mais a sociedade tem precisado se manter conectada virtualmente, aumentando também, como consequência, a quantidade de crimes cibernéticos, com ataques gradativamente mais agressivos e extremos.
A economia global vem sofrendo prejuízo anual de bilhões de dólares com esse aumento de cibercrimes, e a tendência é piorar! Por isso, investir em medidas de proteção é uma solução de emergência!
Portanto, se você é:
• Administrador de rede;
• Desenvolvedor de aplicativos;
• Profissional de segurança;
• Auditor;
• Gerente de qualidade;
• Gerente operacional;
E quer se preparar para ser aprovado no Exame EXIN Cyber & IT Security Foundation,

ESTE LIVRO É PARA VOCÊ!

# Capítulo 1 - Introdução à Segurança Cibernética / Sistemas De Computador

## Arquitetura dos Computadores e Sistemas Operacionais

Para falar sobre a arquitetura dos computadores e sistemas operacionais, precisamos entender o contexto em que foram sendo desenvolvidos e atualizados para atender a constante evolução de necessidades do processo de comunicação cibernético.

## Componentes de Um Sistema de Computação

São considerados componentes de um sistema de computação todas as partes necessárias para seu funcionamento, tanto físicas como lógicas, desde um cabeamento a um aplicativo que possibilite o acesso às redes. Por exemplo:
Hardwares: CPU, chips de memória, dispositivos de armazenamento, dispositivos de entrada e saída, circuito lógico, componentes de segurança, barramentos e componentes de rede;
Softwares: Sistema Operacional, aplicativos;
• Firmwares: Softwares gravados em hardwares (placa de computador, placas de vídeo, etc.);
• Periféricos: Teclados, mouse, impressora, entre outros.
E o controle ou "os controles" de inter-relacionamento entre todas essas partes, podendo usar: multitarefa, multiprocessamento e multithreading.
Uma grande evolução e de bastante utilidade são os dispositivos dedicados, como o Secure Payment para Internet of Things (IoT), o pagamento seguro para Internet das Coisas (IoT). É a mágica de com apenas um toque de botão, os consumidores pagarem pelo gás, comida ou pelo estacionamento, sem sair do carro conectado! Uma forma de incorporar pagamentos seguros em dispositivos conectados, permitindo que qualquer coisa, de um relógio a um carro, inicie os pagamentos... Esse é o conceito Secure Payment para Internet of Things (IoT)! Lembrando que, assim como outros, por mais maravilhoso que seja, é um sistema que precisa de recursos especiais de segurança!
Na verdade, a internet tem ampliado um cenário de recursos cada vez maior para as comunicações, inclusive as pessoais, lançando novas formas de interação para os usuários e evoluindo as já existentes, com atualizações de versões que atendem às necessidades desse progresso, incluindo as soluções de segurança, que sabemos serem necessárias e emergenciais.
Podemos citar como exemplos desses recursos em constante expansão: mensagens de texto, mensagens instantâneas (IM), chats, conferências de áudio, de vídeo e a tecnologia revolucionária de voz sobre IP (VoIP), que chegou para facilitar ainda mais a forma de se

comunicar, reduzindo custos, possibilitando ligações através das redes IP da internet.
Por isso, precisamos entender melhor os elementos e seus papeis dentro da arquitetura da computação e dos sistemas operacionais que proporcionam todos esses recursos cibernéticos.

## A Evolução dos Sistemas Operacionais

A evolução da internet mudou a forma das pessoas se comunicarem e fazerem negócios, trazendo muitas oportunidades e benefícios. E continua a crescer de maneiras inovadoras e variadas, propiciando e otimizando produtos e serviços. Mas essa evolução traz desafios e comportamentos questionáveis que resultam em vulnerabilidades, riscos e ameaças.
A origem da internet está enraizada na ARPANET; sigla de Advanced Research Projects Agency Network, uma rede de computadores que o departamento de defesa dos Estados Unidos criou no ano de 1969. Mas, de lá para cá, a forma como as pessoas usam a internet mudou, descentralizou, não é mais controlada por um governo e nem por nenhuma autoridade cibernética. É uma terra sem dono, em que todos são usuários e cada um que cuide de proteger o seu território e seus pertences! As ameaças estão em constante evolução. Ataques cada vez mais agressivos são praticados por cibercriminosos que conectam seus computadores ou dispositivos à internet para acessar, sequestrar, roubar dados e informações valiosas. Esse cenário agrava ainda mais no âmbito do comércio eletrônico, sendo uma ameaça para a economia nacional. E é por isso que estamos aqui, nos capacitando para fazer a diferença! O mundo precisa de pessoas que entendam de sistemas operacionais para ter como protegê-los.
Mas a internet não teria essa expansão com base apenas em seus bilhões de usuários. É preciso que existam mecanismos para vincular documentos e recursos em computadores. Ou seja, um usuário de um computador "A" precisa de uma forma para abrir um documento do computador "B". Essa necessidade é que deu origem ao sistema WWW, sigla de World Wide Web, que define como os documentos e recursos se relacionam nas máquinas da rede; é a nossa popular WEB! Também conhecida como ciberespaço. A WEB, portanto, é responsável por conectar os computadores da rede a sites, páginas e conteúdos digitais. Podemos afirmar que a WEB é composta por todos os usuários, redes, páginas e aplicativos interconectados neste mundo eletrônico. ão são automaticamente seguros. Os usuários não são todos confiáveis. Então podemos pensar: Se a internet é tão insegura, por que se tornou essa revolução extraordinária de forma tão rápida? É que o crescimento da WEB, desde a década de 1990 até os dias atuais, além de impulsionar recursos e otimizar demandas, possibilitou uma incrível redução de custos nas comunicações de alta velocidade. Portanto, comprovados os benefícios do ciberespaço para as comunicações e negócios, o que nos resta é buscar soluções para os gargalos que assombram essas conexões.

## Como Funciona um Sistema Operacional?

Precisamos ter em mente que os sistemas operacionais gerenciam:
Componentes de hardware;
• Memória;
• Operações de I / O;
• Sistema de arquivos;
• Serviços do sistema;
• Processos (Lembrando que um processo é uma coleção de instruções e recursos atribuídos que estão realmente em execução, ou seja, carregados na memória e ativados pelo sistema operacional).

## Principais Sistemas Operacionais

Entre as principais famílias de sistemas operacionais, podemos citar:
• Unix / Linux;
• Windows;
• iOS / OS X;
• Android;
• z / OS ez / VM.
E entre os principais tipos de arquitetura de um sistema operacional, temos:
• A monolítica, em que todas as funções do negócio são implementadas em um único processo;
• A arquitetura em camadas, ou multicamadas, que é um sistema cliente/servidor (C/S), que trata de forma separada, dividindo o processo em camadas ou domínios de apresentação, processamento de aplicativos e gerenciamento de dados.

## Segurança nos Sistemas de Computador

Para proteger algo precisamos conhecer o que estamos protegendo e de que estamos protegendo. Para cuidar da segurança da arquitetura dos computadores e dos sistemas operacionais, precisamos conhecer a composição de uma infraestrutura típica de TI, com suas vulnerabilidades, ameaças e riscos, para, assim, termos como adotar estratégias adequadas de mitigação.

## Riscos, Ameaças e Vulnerabilidades

• Quando um ativo está exposto a alguma probabilidade de uma ação ruim, temos um **RISCO!**
Lembrando que o termo "ativo", em segurança da informação, é algo de valor para o negócio e para a organização, como por exemplo: um computador, um banco de dados, uma informação, entre outros. E, nesse contexto,

podemos exemplificar como riscos: uma perda de dados, uma perda do negócio devido a um desastre físico tipo a destruição do prédio em que era alocado, o descumprimento de leis e regulamentos, entre outros.

• Quando um ativo pode ser danificado por alguma ação, temos uma AMEAÇA!

As ameaças podem ser naturais ou conduzidas por humanos. São exemplos de ameaças naturais: terremotos, tempestades, incêndios. E as organizações precisam ter planos para garantir que a operação comercial não seja interrompida a fim de que a organização tenha como se recuperar dos danos sofridos.

• Um PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP) objetiva a continuidade das funções da organização.

• Já um PLANO DE RECUPERAÇÃO DE DESASTRES (DRP), é o que define como a organização pode se recuperar após um desastre.

As ameaças causadas por humanos geralmente possuem como alvo os sistemas de computador, e incluem vírus, malwares e acessos não autorizados.

Vamos aproveitar para alinhar o contexto desses termos, velhos conhecidos nossos e que iremos ver bastante daqui por diante:

• VÍRUS – Programa de computador criado para danificar um sistema, um aplicativo, ou dados.

• MALWARE, ou Código Malicioso – Programa de computador criado para produzir alguma ação maliciosa específica, por exemplo: apagar um disco rígido.

Tanto os vírus quanto os malwares, como bem sabemos, são ameaças que podem prejudicar desde um usuário a um negócio e também uma organização.

• Quando uma falha nos permite perceber uma ameaça, temos uma VULNERABILIDADE!

Ressaltando que uma vulnerabilidade por si só também pode causar efeitos em um ativo. Pense em quando acendemos uma boca de fogão, uma tocha, uma vela, enfim. A iluminação ou o fogo não é algo ruim. Precisamos do fogão aceso para cozinhar, afinal é para isso que os fogões existem! Porém, um fogão com sistema de gás mal instalado dentro de uma copa de uma empresa de TI pode causar um acidente que comprometa as infraestruturas e ativos da organização, ainda mais se a copa for alocada ao lado de um data center! Ou seja, se uma ameaça é percebida é porque deve haver uma vulnerabilidade, que nesse exemplo do fogão seria o sistema de gás mal instalado, transformando o fogão em uma ameaça de risco.

Entre os tipos mais comuns de vulnerabilidades, podemos citar:

Em hardwares:

• Exemplos: emanações, vírus do setor de inicialização, canais secretos.

E em sistemas operacionais:

• Exemplos: vírus, worm, Trojan, cryptoware.

Os dispositivos de computador dedicados – usados para pagamento seguro, gerenciamento de chaves, gateways de segurança e "Internet das Coisas",

frequentemente são projetados com pouca segurança e precisam de recursos especiais de segurança.
Entre os tipos mais comuns de vulnerabilidades, podemos citar:
Em hardwares:
• Exemplos: emanações, vírus do setor de inicialização, canais secretos.
E em sistemas operacionais:
• Exemplos: vírus, worm, Trojan, cryptoware.
Os dispositivos de computador dedicados – usados para pagamento seguro, gerenciamento de chaves, gateways de segurança e "Internet das Coisas", frequentemente são projetados com pouca segurança e precisam de recursos especiais de segurança.

**Exemplos de Medidas de Segurança de Sistemas de Computador**

Entre as principais medidas de segurança relacionadas aos sistemas de computador, podemos exemplificar:
• Acesso à memória com recursos de criptografar e descriptografar em tempo real;
• Suporte para uso de smartcard;
• Sensores de detecção de violação;
• Recursos de inicialização segura, ou secure boot;
• Conexão por meio de uma malha física;
• Bateria lógica.

**Exemplos de Medidas de Segurança de Sistemas Informáticos**

E como exemplo dessas medidas de segurança relacionadas com sistemas informáticos, podemos citar:
• Para hardwares: smartcards, inicialização segura, redundância (RAID), backup, consciência de segurança;
• Para sistemas operacionais: antimalware, firewall, gerenciamento de patch, monitoramento, conscientização de segurança;
• Para redes: zonas desmilitarizadas (DMZs), que são sub-redes que ficam entre a rede interna e a Internet, um servidor proxy, firewalls - sem estado, com estado, proxy, e outros -, Bastion Host, e também detecção e prevenção de intrusão.

**Princípios da Tríade A-I-C nas Infraestruturas de TI**

Seja em uma empresa de pequeno porte ou em algum órgão governamental de grande proporção, em qualquer tipo de organização, uma infraestrutura de TI geralmente é composta por sete domínios, que são:
1. Domínio do Usuário;
2. Domínio da Estação de Trabalho;
3. Domínio LAN;
4. Domínio LAN-para-WAN;
5. Domínio WAN;
6. Domínio de Acesso Remoto;

7. Domínio Sistema/Aplicativo.
Importante saber que cada domínio tem suas composições e seus controles de segurança específicos, porém, todos devem atender aosrequisitos da Tríade A-I-C, o tripé dos princípios básicos da segurança da informação.
A Tríade A-I-C defende que atendendo aos princípios de integridade, confidencialidade e disponibilidade é possível garantir que os dados e informações sejam confiáveis.
E quando a organização projeta e utiliza os controles de segurança nos sete domínios de sua infraestrutura de TI atendendo a um ou mais dos princípios da Tríade A-I-C, encontra soluções mais assertivas para mitigar os riscos, ameaças e vulnerabilidades, conseguindo assim um controle mais eficiente de proteção de dados e informações.
Vale saber que você poderá encontrar em algumas literaturas a referência à Tríade A-I-C como "Tríade C-I-A", mas como remete à "CIA" da Agência Central de Inteligência dos Estados Unidos, preferimos seguir a maioria e adotar a nomenclatura de "Tríade A-I-C".
E vamos a esses três princípios que formam o tripé desse triângulo base da segurança da informação que propicia a integridade dos sistemas de TI:

**Integridade**

O princípio da integridade trata da validade e precisão dos dados; visa proteger com exatidão os dados e informações em sua forma íntegra, para que não ocorram modificações não autorizadas; nem por pessoas ou processos não autorizados e nem por pessoas ou processos autorizados! O dado precisa ser mantido em exata consistência. Qualquer modificação de dados não autorizada, por mais que tenha sido de forma acidental e não proposital, é considerada uma violação da integridade dos dados! E dados que não são precisos ou não são válidos, são considerados dados inúteis.
Lembrando que para algumas organizações, dados e informações são considerados ativos de propriedade intelectual, como: patentes, direitos autorais, fórmulas secretas, bancos de dados de clientes, entre outros que podem representar
grande valor para a empresa. É por isso, que não podem ser modificados sem a devida autorização de seus proprietários; sabotagens na integridade dos dados podem causar danos irreparáveis para o negócio!

**Portanto, não esqueça:**
Os dados são considerados íntegros se:
• Não forem alterados;
• Forem válidos;
• Forem precisos.

## Confidencialidade

O princípio da confidencialidade trata a informação de modo que não
seja repassada para processos, pessoas ou entidades não autorizadas. É a exclusividade que limita quem pode ter acesso a um determinado dado ou informação, incluindo dados privados de pessoas físicas, propriedades intelectuais de empresas, segurança nacional entre países e governos.
Com a expansão do e-commerce, cada vez mais usuários fazem compras online, e, para isso, fornecem dados privados para os cadastros e pagamentos. Entre os principais elementos que constituem a identidade de uma pessoa, podemos citar:
• Nome completo;
• Endereço de chegada;
• Data de nascimento;
• Número da Segurança Social;
• Nome do banco;
• Número da conta de banco;
• Número da conta do cartão de crédito;
• Número da conta da concessionária;
• Número da conta da hipoteca;
• Número da apólice de seguro;
Números de contas de títulos e investimentos, entre outras informações que, se um cracker tiver acesso resultará em uma ameaça que se estende a riscos de, além de perdas financeiras, roubo de identidade, e danos ao CPF da vítima, podendo prejudicar ainda a sua classificação de crédito, impossibilitando a obtenção de empréstimos bancários, cartões de crédito, quem sabe até levar anos para limpar o histórico de crédito pessoal.

## Controles de Segurança que Garantem a Confidencialidade

As leis obrigam as organizações a usarem controles de segurança para proteger os dados privados dos clientes. Lembrando que controles de segurança são ações que mitigam riscos. Como por exemplo:
• Treinamentos de segurança para conscientizar os funcionários;
• Política de Segurança de TI bem estruturada, tipo um manual de instruções de controles de segurança;
• Adotar soluções de segurança para as infraestruturas de TI com projeção em camadas, afinal, sabemos que quanto maior o número de camadas, ou de compartimentos, maior a possibilidade de bloqueio e proteção de dados e de propriedades intelectuais, mitigando assim os riscos de ataques e roubos;
• Avaliações periódicas de segurança, realizando testes de invasão (pentest) em sites e nas infraestruturas de TI. É a forma que os profissionais de segurança checam se os controles estão instalados de forma correta;
• Monitorar pontos de entrada e de saída das redes de internet;

• Antivírus nas estações de trabalho e nos servidores;
• Controles de acesso rigorosos, com ID de logon e senhas, para os aplicativos, sistemas e dados. Lembrando que IDs de logon e senhas são apenas verificação de usuário e que é preciso validar os acessos fazendo uma segunda verificação da identidade dos usuários.
Reduzindo os pontos fracos dos softwares nos computadores e nos servidores, fazendo a atualização com patches e com correções de segurança, temos como manter seguros e atualizados nossos sistemas operacionais e nossos aplicativos.
É protegendo os dados que podemos garantir a confidencialidade deles! Para isso, as organizações devem usar controles específicos, do tipo:
• Definição de políticas, procedimentos, padrões e diretrizes de proteção, que indiquem como toda a organização deve lidar com os dados privados;
• Adotar padrões de classificação dos dados para que se possa definir como devem ser tratados, pois assim é possível saber que tipos de controle precisamos para mantê-los seguros;
• Aplicar limites de acesso a dados confidenciais armazenados nos sistemas e aplicativos, permitindo acessar apenas quem for autorizado;
• Criptografar os dados confidenciais e mantê-los ocultos para os usuários não autorizados, principalmente os dados que navegam na internet, mas também os que ficam armazenados nos bancos de dados e dispositivos de armazenamento.

E, para encerrar essa abordagem sobre confidencialidade, vale reforçar uma orientação que todo mundo deve saber e que não pode deixar de ser seguida:
Nunca inserir dados privados em texto simples, sem criptografia, em e-mails e sites não confiáveis; e nunca inserir dados privados em sites ou aplicativos que não usam criptografia!

**Disponibilidade**

O princípio da disponibilidade é a propriedade que trata de fazer com que os dados ou as informações estejam disponíveis, acessíveis e utilizáveis para uso e manuseio em uma demanda devidamente autorizada.
As características do princípio de disponibilidade são:
• Pontualidade. Os sistemas de informação estão disponíveis quando necessários;
• Continuidade. O pessoal pode continuar trabalhando em casos de falhas ou indisponibilidade;
• Robustez. Capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.

## Métricas da Disponibilidade

Se pararmos para refletir, perceberemos que a disponibilidade é um termo bem comum em nosso dia a dia. Por exemplo: quando você liga para um amigo e o convida para assistir um filme na TV na sua casa. O serviço do telefone, da TV, e até o seu amigo precisam estar disponíveis para que o encontro aconteça como esperado; desde a ligação para o convite até o final do filme. No contexto da segurança da informação não é diferente; o termo disponibilidade também se refere à quantidade de tempo que os usuários podem utilizar um sistema, um aplicativo e dados. Com essa referência que relaciona a disponibilidade ao tempo de uso, temos medidas ou fatores comuns que incluem:

• TEMPO DE ATIVIDADE, que é a quantidade total de tempo acessível de um sistema, aplicativo e dados, geralmente medido em unidades de segundos, minutos e horas dentro de um mês determinado;

• TEMPO DE INATIVIDADE, que é justamente o oposto, ou seja, é a quantidade total de tempo inacessível. Com medição também feita em unidades de segundos, minutos e horas em um mês;

• TEMPO MÉDIO DE FALHA (MTTF), que é a média do intervalo de tempo entre falhas de um sistema específico. Podemos exemplificar essa medição com semicondutores e eletrônicos, que não quebram e, por isso, possuem um MTTF de 25 anos ou mais. Já algumas peças físicas como: conectores, ventiladores, cabos, fontes de alimentação e outras, por sofrerem mais desgastes, possuem uma MTTF bem menor, por volta de uns cinco anos ou menos;

• TEMPO MÉDIO DE REPARO (MTTR), que é a quantidade média de tempo que se gasta para reparar um componente, um aplicativo, ou um sistema.

Essa medida existe para ajudar na agilidade de recuperação do sistema;

• OBJETIVO DE TEMPO DE RECUPERAÇÃO (RTO), que é a quantidade de tempo gasta para recuperar e disponibilizar dados, aplicativos e sistemas após sofrerem alguma interrupção. Planos de continuidade de negócios geralmente definem RTO para acesso a dados, a aplicativos e sistemas de missão crítica;

• DISPONIBILIDADE, que é o cálculo matemático feito em fração:

D = (Tempo total de atividade) / (Tempo total de atividade + Tempo total de inatividade).

Graças a essas métricas é que empresas de telecomunicações podem oferecer aos clientes os famosos SLAs, que bem sabemos ser os queridos acordos de nível de serviço. Na prática, um SLA acontece em forma de um contrato, garantindo a disponibilidade mensal mínima de serviços para redes de longa distância (WAN) e para links de acesso à internet. Na verdade, os SLAs são verdadeiros parceiros dos serviços WAN e dos links de acesso dedicado à internet! E o fator disponibilidade mede exatamente esse nível de serviço de tempo das atividades mensais. Geralmente, provedores de serviços oferecem SLAs com disponibilidade entre 99,5% a 99,999%

## Estrutura da Política de Segurança de TI

Sabendo que a segurança de TI é fundamental para a capacidade de sobrevivência de qualquer organização, surge a necessidade de uma estrutura da política de segurança de TI, que consiste nas políticas, padrões, procedimentos e diretrizes que reduzem os riscos e as ameaças.

O objetivo da estrutura da política de segurança de TI da organização é reduzir a exposição a riscos, ameaças e vulnerabilidades.

Na prática, uma estrutura de política de segurança de TI tem quatro componentes. São eles:

• POLÍTICA - Uma política é uma breve declaração escrita, registrando que as pessoas responsáveis por uma organização definiram um curso de ação ou direção. Uma política é determinada pela alta administração para ser aplicada a toda organização;

• PADRÃO - Um padrão é uma definição escrita detalhada de como devem ser utilizados os hardwares e softwares da organização. Os padrões garantem que os controles de segurança adotados sejam usados em todo o sistema de TI;

• PROCEDIMENTOS - São instruções escritas sobre como usar as políticas e os padrões, incluindo: plano de ação, instalação, teste e auditoria dos controles de segurança;

• DIRETRIZES - Uma diretriz é um curso de ação sugerido para usar a política, padrões ou procedimentos. As diretrizes podem ser específicas ou flexíveis quanto ao uso.

É importante saber diferenciar e relacionar a definição de política e de padrão para os requisitos práticos de design; requisitos esses que devem ser aplicados de forma adequada aos controles de segurança e contramedidas. As declarações de política devem definir limites e também se referir aos padrões, procedimentos e diretrizes. As políticas definem como os controles de segurança e as contramedidas devem ser usadas para cumprir as leis e os regulamentos.

• CONTRAMEDIDA, ou "salvaguarda" - É uma medida de segurança que se coloca em prática para mitigar um risco potencial. Como por exemplo: gerenciamento de senha forte; controles de acesso em sistemas operacionais, implementação de senhas do BIOS (sistema básico de entrada e saída), treinamentos sobre segurança, entre outras.

Normalmente, após realizada uma avaliação de segurança no sistema de TI de uma organização, as definições de política são alinhadas às lacunas e exposições. As políticas devem exigir revisão e aprovação da gerência executiva e do conselho jurídico geral. A estrutura da política de segurança de TI deve começar a ser definida a partir de uma política de classificação de ativos, que, por sua vez, deve ser alinhada a um padrão de classificação de dados.

### Padrões de Classificação de Dados

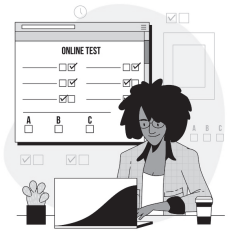
O padrão de classificação de dados define como a organização deve proteger seus dados. É a partir do padrão de classificação de dados que se deve avaliar se há tráfego de dados privados ou confidenciais em qualquer um dos sete domínios de uma infraestrutura típica de TI. E, dependendo de como os dados são classificados é que são determinados os devidos controles de segurança.
Portanto, o objetivo/meta de um padrão de classificação de dados é: definir, de forma consistente, como a organização deve tratar e proteger seus diferentes tipos de dados.
Os controles de segurança variam de acordo com as necessidades de proteção dos diferentes dados. Por isso, cada domínio da infraestrutura de TI deve ter seus controles de segurança com procedimentos e diretrizes específicos, para lidar com os dados dentro de cada um deles.
De acordo com as regulamentações recentes dos padrões de classificação de dados, podemos diferenciá-los em quatro principais categorias:
• Dados privados, que são os dados sobre pessoas, e que devem ser mantidos em sigilo;
• Confidencial, que são informações ou dados de propriedade da organização. Como por exemplo: propriedade intelectual, listas de clientes, informações sobre preços e patentes;
• Apenas para uso interno, que são as informações ou dados armazenados internamente por uma organização;
• Dados de domínio público, que são Informações ou dados compartilhados com o público, como: conteúdos de sites, White papers, entre outros.
O padrão de classificação de dados da organização vai definir se é necessário ou não usar a criptografia, que geralmente é usada nos dados mais sensíveis, mesmo em dispositivos de armazenamento e discos rígidos.

# Usuário – O ponto mais fraco na segurança de uma infraestrutura de TI!

Sim... o usuário é o elo mais fraco na segurança de ativos de uma organização. E não só os usuários comuns, mas até mesmo os profissionais de segurança de sistemas de informação cometem erros!
O erro humano é o maior risco e a maior ameaça para qualquer organização, porque nenhuma organização pode controlar totalmente o comportamento dos seus funcionários.

Por isso, toda organização, por melhor que seja o departamento de Recursos Humanos em seus cuidados na contratação e gestão de pessoas, precisa estar preparada para usuários mal-intencionados, usuários não treinados e usuários descuidados.
Nem sempre o erro será intencional, mas causará danos do mesmo jeito! Por isso, estratégias precisam ser elaboradas e utilizadas para ajudar a reduzir os riscos, como por exemplo:
• Verificar cuidadosamente o histórico de cada candidato, antes que seja contratado;
• Efetuar avaliações regulares com todos os membros da equipe;
• Alternar o acesso a sistemas, aplicativos e dados confidenciais com diferentes cargos da equipe, usando uma escala de confidencialidade;
• Aplicar testes e análise de qualidade nos softwares, aplicativos e sistemas;
• Revisar regularmente os planos de segurança em toda infraestrutura de TI.
Lembrando que uma política de segurança bem elaborada e devidamente aplicada é a melhor forma de prevenção de riscos!

# Pratique o que Aprendeu




Que tal colocar em prática o que você aprendeu até aqui? Para isso, aproveite esses exercícios de fixação:

**1. São componentes de um sistema de computação, exceto:**

a) Software
b) Firmware
c) Hardware
d) Malware

**2. Sobre o funcionamento de um sistema operacional, podemos afirmar que:**

a) Os sistemas operacionais gerenciam componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
b) Os sistemas operacionais apenas desenvolvem componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
c) Os sistemas operacionais gerenciam apenas redes e protocolos.
d) Os sistemas operacionais funcionam apenas com componentes lógicos.

**3. Entre os principais sistemas operacionais, podemos citar:**

a) TCP/IP, Windows, iOS / OS X, Android, z / OS ez / VM.
b) Unix / Linux, Windows, iOS / OS X, Android, IPSec.
c) Unix / Linux, Windows, IPv4/IPv6, Android, z / OS ez / VM.
d) Unix / Linux, Windows, iOS / OS X, Android, z / OS ez / VM.

**4. Assinale a alternativa que não representa um tipo de vulnerabilidade de sistemas de computador:**

a) Emanações em hardware.
b) Vírus em sistemas operacionais.
c) IPSec.
d) Pouca segurança em dispositivos dedicados.

**5. São medidas de segurança relacionadas a sistemas de computador, exceto:**

a) Acesso à memória com recursos de criptografar e descriptografar em tempo real.
b) Suporte para uso de smartcard.
c) Sensores de detecção de violação.
d) Canais secretos.

**6. Se a internet é tão insegura, por que se tornou um meio de comunicação extraordinário de forma tão rápida?**

a) Porque além de impulsionar recursos e otimizar demandas, possibilitou uma incrível redução de custos nas comunicações de alta velocidade.
b) Porque viralizou e acabou expandindo para o público geral.
c) Porque houve uma manipulação governamental política com objetivos de controle social.
d) Porque foi parte de um planejamento de organizações privadas destinadas a comandar e manipular a massa midiática.

**7. Por que o usuário é considerado o ponto mais fraco na segurança de uma infraestrutura básica de TI de uma organização?**

a) Porque os erros em uma infraestrutura de TI em uma organização não são intencionais, e errar é uma vulnerabilidade inerente a todo ser humano.
b) Porque sempre são vítimas de acusações por parte da administração.
c) Porque nenhuma organização pode controlar totalmente o comportamento dos seus funcionários.
d) Porque a maioria dos usuários de uma organização não possui conhecimentos específicos que a torne mais ativa em relação às programações tecnológicas de medidas de segurança.

**8. Quando um ativo está exposto a alguma probabilidade de uma ação ruim, temos (...):**

a) Uma ameaça.
b) Uma vulnerabilidade.
c) Um dano.
d) Um risco.

**9. Plano que objetiva a continuidade das funções da organização:**

a) Plano de Recuperação de Desastres (DRP)
b) Plano de Continuidade de Negócios (BCP)
c) Plano de Segurança Organizacional (PSO)
d) Plano de Correção de Danos (PCD)

**10. Os dados são considerados íntegros se:**

**I. Não forem alterados;**
**II. Forem válidos;**
**III. Forem precisos;**
**IV. Não forem compartilhados.**

a) Apenas as alternativas I e II são verdadeiras.
b) Apenas as alternativas I, II e III são verdadeiras.
c) Todas as alternativas são verdadeiras.
d) Somente a alternativa IV é verdadeira.

# Gabarito de respostas

Confirme suas respostas e aprenda com seus erros e acertos.

**1. São componentes de um sistema de computação, exceto:**

a) Software
b) Firmware
c) Hardware
d) Malware

a) Incorreto. Software é um componente de um sistema de computação.
b) Incorreto. Firmware é um componente de um sistema de computação.
c) Incorreto. Hardware é um componente de um sistema de computação.
**d) Correto. Malware é um código malicioso, não é um componente de um sistema de computação.**

**2. Sobre o funcionamento de um sistema operacional, podemos afirmar que:**

a) Os sistemas operacionais gerenciam componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
b) Os sistemas operacionais apenas desenvolvem componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
c) Os sistemas operacionais gerenciam apenas redes e protocolos.
d) Os sistemas operacionais funcionam apenas com componentes lógicos.

**a) Correto. Os sistemas operacionais gerenciam componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.**
b) Incorreto. Os sistemas operacionais (~~apenas desenvolvem~~) gerenciam componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
c) Incorreto. Os sistemas operacionais gerenciam (~~apenas redes e protocolos~~) componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.
d) Incorreto. Os sistemas operacionais (~~funcionam apenas com componentes lógicos~~) gerenciam componentes de hardware, memória, operações de I / O, sistema de arquivos, serviços do sistema e processos.

**3. Entre os principais sistemas operacionais, podemos citar:**

a) TCP/IP, Windows, iOS / OS X, Android, z / OS ez / VM.
b) Unix / Linux, Windows, iOS / OS X, Android, IPSec.
c) Unix / Linux, Windows, IPv4/IPv6, Android, z / OS ez / VM.
d) Unix / Linux, Windows, iOS / OS X, Android, z / OS ez / VM.

a)Incorreto. (~~TCP/IP~~), Windows, iOS / OS X, Android, z / OS ez / VM.
b) Incorreto. Unix / Linux, Windows, iOS / OS X, Android, (~~IPSec~~).
c) Incorreto. Unix / Linux, Windows, (~~IPv4/IPv6~~), Android, z / OS ez / VM.
d) Correto. Unix / Linux, Windows, iOS / OS X, Android, z / OS ez / VM.

**4. Assinale a alternativa que não representa um tipo de vulnerabilidade de sistemas de computador:**

a) Emanações em hardware.
b)Vírus em sistemas operacionais.
c) IPSec.
d) Pouca segurança em dispositivos dedicados.

a) Incorreto. Emanações em hardware é um tipo de vulnerabilidade sistêmica.
b) Incorreto. Vírus em sistemas operacionais é um tipo de vulnerabilidade sistêmica.
**c) Correto. IPSec é um protocolo de segurança, não é uma vulnerabilidade.**
d) Incorreto. Pouca segurança em dispositivos dedicados é uma vulnerabilidade sistêmica.

**5. São medidas de segurança relacionadas a sistemas de computador, exceto:**

a) Acesso à memória com recursos de criptografar e descriptografar em tempo real.
b) Suporte para uso de smartcard.
c) Sensores de detecção de violação.
d) Canais secretos.

a)Incorreto. Acesso à memória com recursos de criptografar e descriptografar em tempo real é uma medida de segurança sistêmica.
b) Incorreto. Suporte para uso de smartcard é uma medida de segurança sistêmica.
c) Incorreto. Sensores de detecção de violação é uma medida de segurança sistêmica.
**d) Correto. Canais secretos são vulnerabilidades em hardwares.**

**6. Se a internet é tão insegura, por que se tornou um meio de comunicação extraordinário de forma tão rápida ?**

a) Porque além de impulsionar recursos e otimizar demandas, possibilitou uma incrível redução de custos nas comunicações de alta velocidade.
b) Porque viralizou e acabou expandindo para o público geral.
c) Porque houve uma manipulação governamental política com objetivos de controle social.
d) Porque foi parte de um planejamento de organizações privadas destinadas a comandar e manipular a massa midiática.

**a) Correto. Porque além de impulsionar recursos e otimizar demandas, possibilitou uma incrível redução de custos nas comunicações de alta velocidade.**

b) Incorreto. “Porque viralizou e acabou expandindo para o público geral” não é a causa do sucesso da internet, foi uma consequência.
c) Incorreto. “Porque houve uma manipulação governamental política com objetivos de controle social” não é uma causa f undamentada que justifique o sucesso da internet.
d) Incorreto. “Porque foi parte de um planejamento de organizações privadas destinadas a comandar e manipular a massa midiática” não é uma causa fundamentada que justifique o sucesso da internet.

**7. Por que o usuário é considerado o ponto mais fraco na segurança de uma infraestrutura básica de TI de uma organização?**

a) Porque os erros em uma infraestrutura de TI em uma organização não são intencionais, e errar é uma vulnerabilidade inerente a todo ser humano.
b) Porque sempre são vítimas de acusações por parte da administração.
c) Porque nenhuma organização pode controlar totalmente o comportamento dos seus funcionários.
d) Porque a maioria dos usuários de uma organização não possue conhecimentos específicos que a torne mais ativa em relação às programações tecnológicas de medidas de segurança.

a) Incorreto. “Porque os erros em uma infraestrutura de TI em uma organização (~~não são intencionais~~), (~~e errar é uma vulnerabilidade inerente a todo ser humano~~)”. (~~Os erros podem ser intencionais ou não. E o “errar é humano” não representa e não justifica a falta de controle por parte das organizações em relação aos seus funcionários~~).
b) Incorreto. (~~Porque sempre são vítimas de acusações por parte da administração~~). (Afirmação inverídica e que não caracteriza o real motivo).
**c) Correto. Porque nenhuma organização pode controlar totalmente o comportamento dos seus funcionários.**
d) Incorreto. Porque (~~a maioria dos usuários de uma organização não possui conhecimentos específicos que a~~ torne mais ativa em relação às programações tecnológicas de ~~medidas de segurança~~). (Não justifica, pois até funcionários com conhecimentos específicos em programação podem errar, intencionalmente ou não).

**8. Quando um ativo está exposto a alguma probabilidade de uma ação ruim, temos (...):**

a) Uma ameaça.
b) Uma vulnerabilidade.
c) Um dano.
d) Um risco.

a) Incorreto. Uma ameaça existe quando há uma possibilidade de um ativo ser danificado por alguma ação.
b) Incorreto. Uma vulnerabilidade é uma falha que permite perceber uma ameaça.
c) Incorreto. Um dano é a consequência de um evento negativo.
**d) Correto. Um risco.**

**9. Plano que objetiva a continuidade das funções da organização:**

a) Plano de Recuperação de Desastres (DRP)
b) Plano de Continuidade de Negócios (BCP)
c) Plano de Segurança Organizacional (PSO)
d) Plano de Correção de Danos (PCD)

a) Incorreto. Um Plano de Recuperação de Desastres (DRP) é o que define como a organização pode se recuperar após um desastre.
**b) Correto. Plano de Continuidade de Negócios (BCP)**
c) Incorreto. Plano de Segurança Organizacional (PSO) não existe.
d) Incorreto. Plano de Correção de Danos (PCD) não existe.

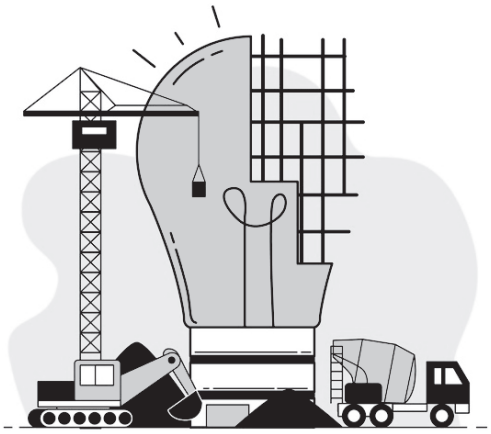
**10. Os dados são considerados íntegros se:**

**I. Não forem alterados;**
**II. Forem válidos;**
**III. Forem precisos;**
**IV. Não forem compartilhados.**

a) Apenas as alternativas I e II são verdadeiras.
b) Apenas as alternativas I, II e III são verdadeiras.
c) Todas as alternativas são verdadeiras.
d) Somente a alternativa IV é verdadeira.

a) Incorreto. As alternativas III também é verdadeira.
**b) Correto. Apenas as alternativas I, II e III são verdadeiras.**
c) Incorreto. A alternativa IV não é verdadeira. Compartilhar um dado não fere a integridade de um dado, desde que não seja alterado, seja válido e preciso.
d) Incorreto. Somente as alternativas I, II e III são as verdadeiras.

# Capítulo 2 - Segurança nas Infraestruturas de TI / Os 7 Domínios



## Os 7 Domínios De Uma Infraestrutura Típica De TI:

1. Domínio do Usuário;
2. Domínio da Estação de Trabalho;
3. Domínio LAN;
4. Domínio LAN-para-WAN;
5. Domínio WAN;
6. Domínio de Acesso Remoto;
7. Domínio Sistema/Aplicativo.

## 1. Domínio do Usuário

O primeiro domínio é o do usuário.
Como a própria nomenclatura sugere, o 'Domínio do Usuário' é o que define quem acessa o sistema de informação de uma organização.

## Como Funciona o Domínio do Usuário?

Quando nos referimos a funções e tarefas dentro de uma empresa, sabemos que seus colaboradores são usuários que podem acessar sistemas, aplicativos e dados de acordo com a escala de autorização. Por isso, todos os funcionários precisam seguir um manual de política organizacional para saber exatamente o que lhe é permitido ou não.
É no domínio do usuário que devemos encontrar uma Política de Uso Aceitável (AUP) para definir o que os usuários estão autorizados a fazer com os ativos de TI da organização; na verdade, essa prática de introdução de uma AUP é uma recomendação legal para a maioria das organizações.  É literalmente instalar o manual de regras! E todos os funcionários devem estar cientes de que violar uma dessas regras pode ser motivo até para demissão! E é exatamente assim que se instala a primeira camada de defesa de uma estratégia de segurança em camadas.

Então, não esqueça:
• A POLÍTICA DE USO ACEITÁVEL (AUP) define quais ações são ou não são permitidas em relação ao uso de ativos de TI de avaliação de ameaça da organização. Lembrando também que trata-se de uma política específica do Domínio do Usuário, usada para reduzir os riscos entre a organização e seus funcionários.
Outra política que também é específica deste domínio é a POLÍTICA DE CONSCIENTIZAÇÃO DE SEGURANÇA, usada quando é preciso alterar o comportamento de conscientização da segurança organizacional. Essa política define como garantir que todos os funcionários da organização estejam cientes da importância da segurança e das expectativas comportamentais de acordo com a política de segurança organizacional.

## Responsabilidades no Domínio do Usuário

Cientes de suas funções, tarefas e permissões, os funcionários podem se responsabilizar pelo uso dos ativos da TI da organização. Por exemplo: A empresa pode exigir que os funcionários, tanto os contratados como os terceirizados, assinem um acordo de compromisso com a manutenção das informações confidenciais. Como também pode incluir a exigência de antecedentes criminais para verificar se há histórico suspeito que possa se transformar em uma ameaça para segurança dos ativos da TI.
Normalmente, é o gerente de departamento ou dos recursos humanos (RH) que fica responsável por garantir que todos os funcionários assinem e cumpram as regras da AUP.
E é o RH que deve checar o perfil e o histórico dos candidatos a funcionários antes que sejam contratados e liberados para acessar e usar os sistemas de TI da organização.
O elo mais vulnerável de uma infraestrutura de TI é o Domínio do Usuário, por isso todos da organização precisam entender o porquê da necessidade do comprometimento com a segurança dos ativos. Para isso existem as:
• POLÍTICA DE CLASSIFICAÇÃO DE ATIVOS, que define o padrão de classificação de dados de uma organização, determina quais ativos de TI são essenciais para a missão organizacional, definindo os sistemas, usos e prioridades de dados, identificando assim os ativos nos sete domínios de uma infraestrutura típica de TI;
• POLÍTICA DE GESTÃO DE ATIVOS, que inclui as operações de segurança e o gerenciamento de todos os ativos de TI nos sete domínios de uma infraestrutura de TI típica.

## Relação: Riscos, Ameaças, Vulnerabilidades X Estratégias de Mitigação no Domínio do Usuário

Vejamos alguns dos riscos, ameaças e vulnerabilidades mais frequentes no domínio do usuário e estratégias de mitigação relacionadas:

| DOMÍNIO DO USUÁRIO | |
|---|---|
| RISCOS, AMEAÇAS E VULNERABILIDADES | ESTRATÉGIAS DE MITIGAÇÃO |
| Falta de consciência do usuário. | Realizar treinamentos de conscientização sobre a importância e como cumprir as medidas de segurança estabelecidas. Podem ser feitas também ações do tipo: cartazes, banners, lembretes, saudações, e-mails, entre outras formas de comunicação interna. |
| Apatia dos usuários quanto às políticas da empresa. | Investir em treinamentos anuais de conscientização. Além de implementar política de uso aceitável, e atualizar sempre que necessário o manual das regras, fazendo avaliações de desempenho periódicas com conversação e feedbacks pontuais. |
| Violações da política de segurança. | Colocar os funcionários em sistema de liberdade condicional, passando por avaliações de desempenho abertas a conversação. E também revisar a AUP e o manual das regras periodicamente. |
| Usuário inserir dispositivos do tipo CDs e drivers USB contendo fotos pessoais, músicas, vídeos, enfim, invadindo o ambiente de TI com componentes pessoais. | Desativar unidades de CD internas, portas USB e qualquer ponto de vulnerabilidade que possibilite esse tipo de evento. Habilitar um antivírus automático nas unidades de mídia relacionadas, checando inclusive e-mails e arquivos anexos. Geralmente, um sistema de varredura antivírus é suficiente para examinar todos os novos arquivos no disco rígido do computador. |

| | |
|---|---|
| Usuário baixar algum arquivo como música, foto ou vídeo. | Habilitar a filtragem de conteúdo, aplicar antivírus, verificando arquivos, anexos em e-mails e mídias relacionadas. Configurar dispositivos de rede de filtragem de conteúdo de acordo com a definição da AUP para negar ou permitir nomes de domínio específico. |
| A organização sofrer ataques ou sabotagens feitos por funcionários descontentes | Rastrear e monitorar comportamentos suspeitos dos funcionários, performances de trabalho irregulares e uso da infraestrutura de TI fora do expediente. E, de acordo com esse monitoramento e com base na AUP, dar início aos procedimentos de bloqueio em relação ao controle de acesso de TI. |
| Romance quando acaba entre funcionários da empresa. | Monitorar e rastrear comportamentos fora do padrão, inclusive o uso da infraestrutura de TI fora do horário de trabalho. E, dar início aos procedimentos de bloqueio em relação ao controle de acesso de TI, de acordo com o monitoramento e com base na AUP. |

| | |
|---|---|
| Chantagem ou extorsão por parte de funcionários da empresa. | Monitorar e rastrear comportamentos fora do padrão e o uso da infraestrutura de TI fora do horário de trabalho. Habilitar o sistema de detecção de intrusão (IDS) e o sistema de prevenção de intrusão (IPS) para monitorar acessos e ações pessoais dos funcionários dentro da infraestrutura de TI da empresa. Lembrando que o IDS e o IPS são dispositivos de segurança que monitoram os fluxos de dados IP no tráfego de entrada e de saída, e que podem ter alertas e alarmes programados para ajudar a detectar e bloquear tráfegos considerados suspeitos de acordo com a definição da AUP. |

**2. Domínio da estação de trabalho.**

O segundo domínio é o da estação de trabalho. É onde a maioria dos usuários de uma organização se conecta à infraestrutura de TI.
Podemos entender como estação de trabalho:
• Computador;
• Laptop;
• Assistente de Dados Pessoais (PDA);
• Smartphone;
• Qualquer dispositivo que possibilite acesso à rede.

**Como funciona o Domínio da Estação de Trabalho?**

Para que haja produtividade em uma organização é preciso que a equipe tenha o acesso necessário à infraestrutura de TI.
Entre as tarefas relacionadas ao Domínio da Estação de Trabalho, podemos citar:
• Configuração de hardware;
• Sistemas de proteção;
• Checagem de arquivos de antivírus.