



FIAP

Fundamentos de Segurança Cibernética

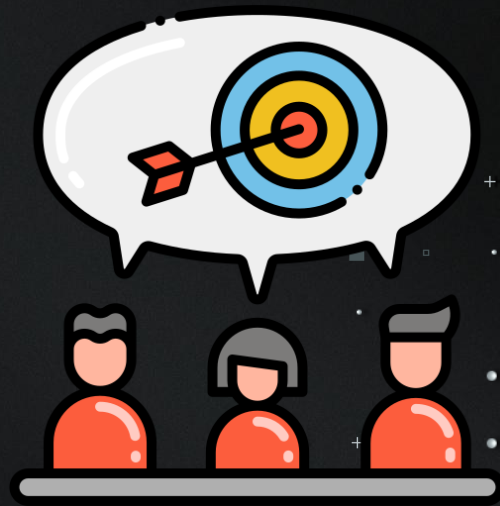
Introdução à Segurança Cibernética

Prof. MSc. Oerton Fernandes

Introdução à Segurança Cibernética e Histórico de Ataques Cibernéticos

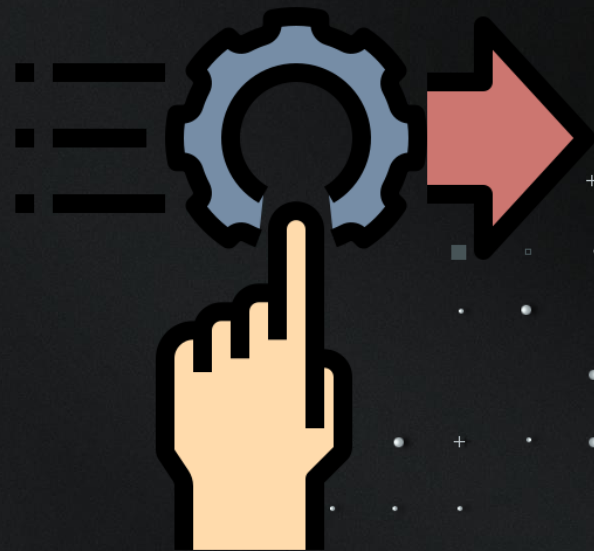
Objetivo: Introduzir os conceitos básicos de segurança cibernética e apresentar exemplos históricos de ataques cibernéticos.

- ❌ Conceitos de segurança cibernética.
- ❌ Importância da segurança cibernética.
- ❌ Exemplos históricos de ataques cibernéticos.



Atividade Prática

- ❖ Apresentar o *iptables* e o Windows Firewall.
- ❖ Demonstrar a configuração de regras básicas no firewall.
- ❖ Configurar suas próprias regras, permitindo apenas conexões SSH e HTTP.





O que é Segurança da Informação?

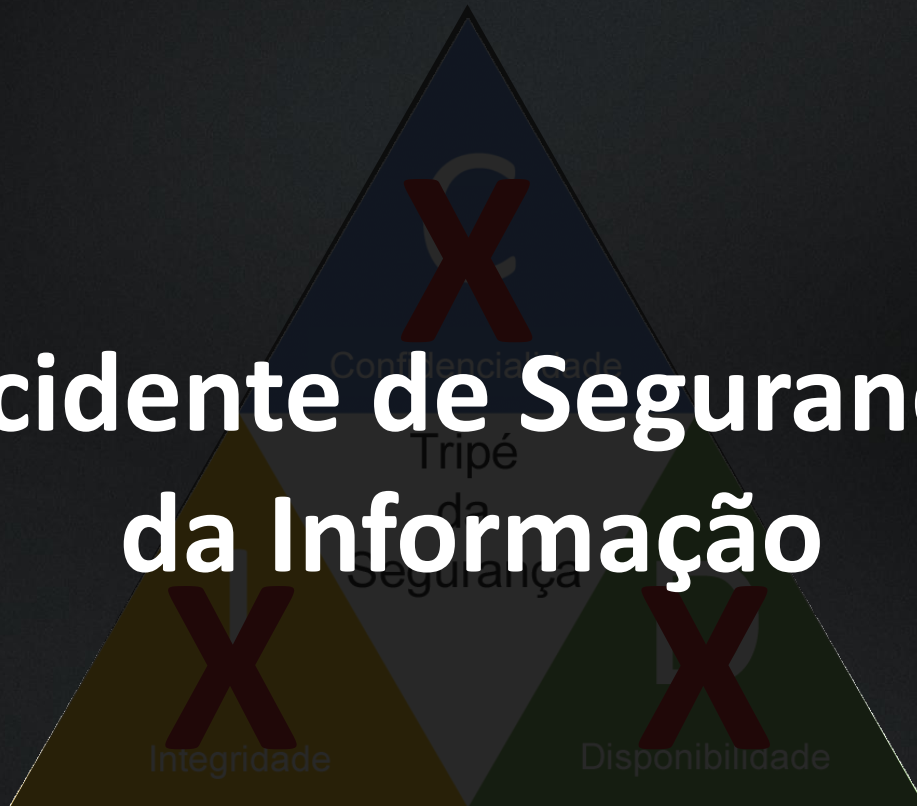


É a proteção de informações contra **qualquer** tipo de ameaça, com o objetivo de **garantir** a **continuidade** dos **negócios**, **minimizar** danos e **maximizar** o retorno sobre os investimentos e as oportunidades.





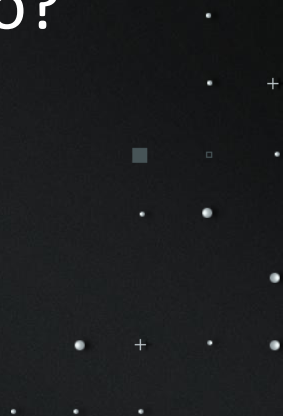
Incidente de Segurança da Informação

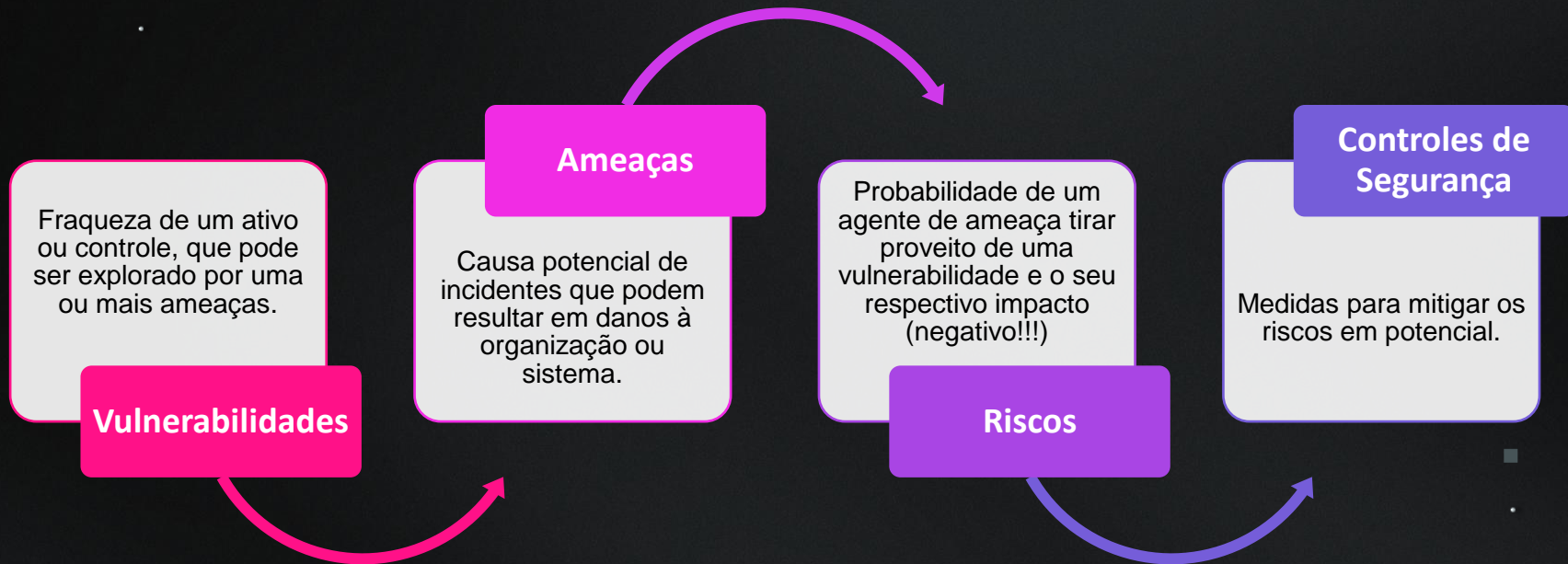


Fundamentos de Segurança Cibernética



O **que** estamos protegendo e **do**
que estamos protegendo?







**Segurança
Física**



**Segurança
Técnica**



**Segurança
Organizacional**

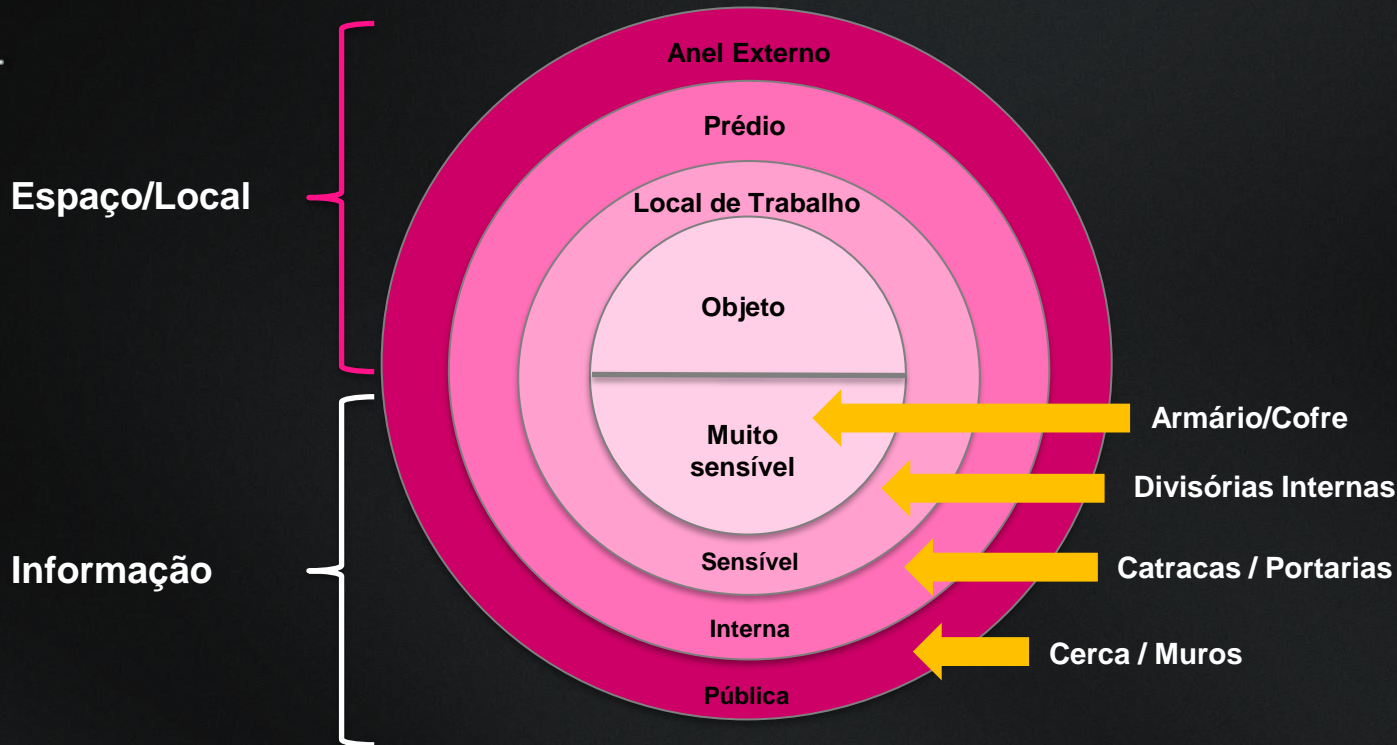


**Segurança
Física**

Proteger seus **ativos físicos** – tanto materiais quanto os menos tangíveis – de ameaças físicas:

- ❌ Acesso não autorizado;
- ❌ Indisponibilidades e danos causados por ações humanas;
- ❌ Eventos ambientais e externos.

Onde começam as medidas?





Segurança
Técnica

Implementação de medidas para proteger as informações e sistemas de uma organização contra:

- ❌ Acesso **lógico** não autorizado;
- ❌ Vazamento de informações e dados;
- ❌ Danos potências a sistemas, informações e dados.



Segurança
Organizacional

Implementação de **políticas, normas, processos** e **estruturas organizacionais** necessárias para **proteger** as informações contra **ameaças** e **garantir** a continuidade dos negócios.



O que é um Firewall?

Firewall

Firewall é uma **ferramenta de segurança** de rede que **monitora** e **controla** o tráfego de rede, **permitindo** ou **bloqueando** pacotes de dados com base em um conjunto definido de regras de segurança.



FIAP

- ❌ Protegem contra ameaças externas;
- ❌ Controlam o acesso
- ❌ Monitoram tráfegos de dados e informações

Analisam **pacotes de dados individualmente**, permitindo ou bloqueando com base em **regras predefinidas**, como endereços IP, portas e protocolos.



Monitoram o **estado das conexões de rede**,
permitindo ou bloqueando pacotes com base no
estado e contexto da conexão.



Atuam como **intermediários** entre os **dispositivos** da **rede** e a **internet**, **filtrando** todo o tráfego de rede e **inspecionando** o conteúdo dos pacotes.





Integram **funcionalidades avançadas**, como **inspeção** profunda de pacotes, **prevenção** contra intrusões (IPS), **controle** de aplicativos e **integração** com sistemas de inteligência de ameaças.



Projetados especificamente para **proteger aplicações web**, monitorando e filtrando o tráfego HTTP/HTTPS.

A rede social LinkedIn sofreu uma invasão que expôs os dados pessoais de mais de **117 milhões de usuários**. O ataque explorou uma **vulnerabilidade** no firewall da empresa, **permitindo** o acesso a senhas e outros dados pessoais.



- ❌ **Invalidaram** as senhas de todos os usuários que não haviam alterado suas senhas desde 2012
- ❌ **Incentivaram** todos os usuários a alterarem suas senhas.
- ❌ **Implementaram** o uso de *salting* nas senhas para aumentar a segurança



O Banco Neon sofreu um **vazamento de dados** que **levantou** questões urgentes sobre a segurança cibernética no setor financeiro. O vazamento envolveu a **cópia não autorizada de dados de parte dos seus clientes**, que não permitia acessar as contas bancárias nem realizar transações. A instituição tomou medidas para cessar quaisquer acessos indevidos e está investigando o ocorrido.



FIAP

Fundamentos de Segurança Cibernética

Exemplos Históricos de Incidentes



neon

O Yahoo anunciou um **vazamento de dados** que afetou **3 bilhões de contas**. A falha no **firewall** permitiu que os invasores **acessassem informações** como nomes, telefones, datas de nascimento e senhas.





- ❌ **Invalidaram** as perguntas de segurança não criptografadas;
- ❌ **Exigiram** que todos os usuários alterassem suas senhas, especialmente se não tivessem feito isso desde 2013;
- ❌ **Implementaram** o uso do algoritmo *bcrypt* para *hashing* das senhas (mais seguro).

Atividade Prática

- ✖ Apresentar o *iptables* e o Windows Firewall.
- ✖ Demonstrar a configuração de regras básicas no firewall.
- ✖ Configurar suas próprias regras, permitindo apenas conexões SSH e HTTP.

É uma ferramenta de **linha de comando** usada para **configurar**, **gerenciar** e **inspecionar** as regras de firewall do *netfilter* no kernel do Linux. Amplamente utilizada para **implementar regras** de **filtragem** de **pacotes**, **NAT** (*Network Address Translation*) e **gerenciamento** de **conexões** de rede em sistemas Linux.



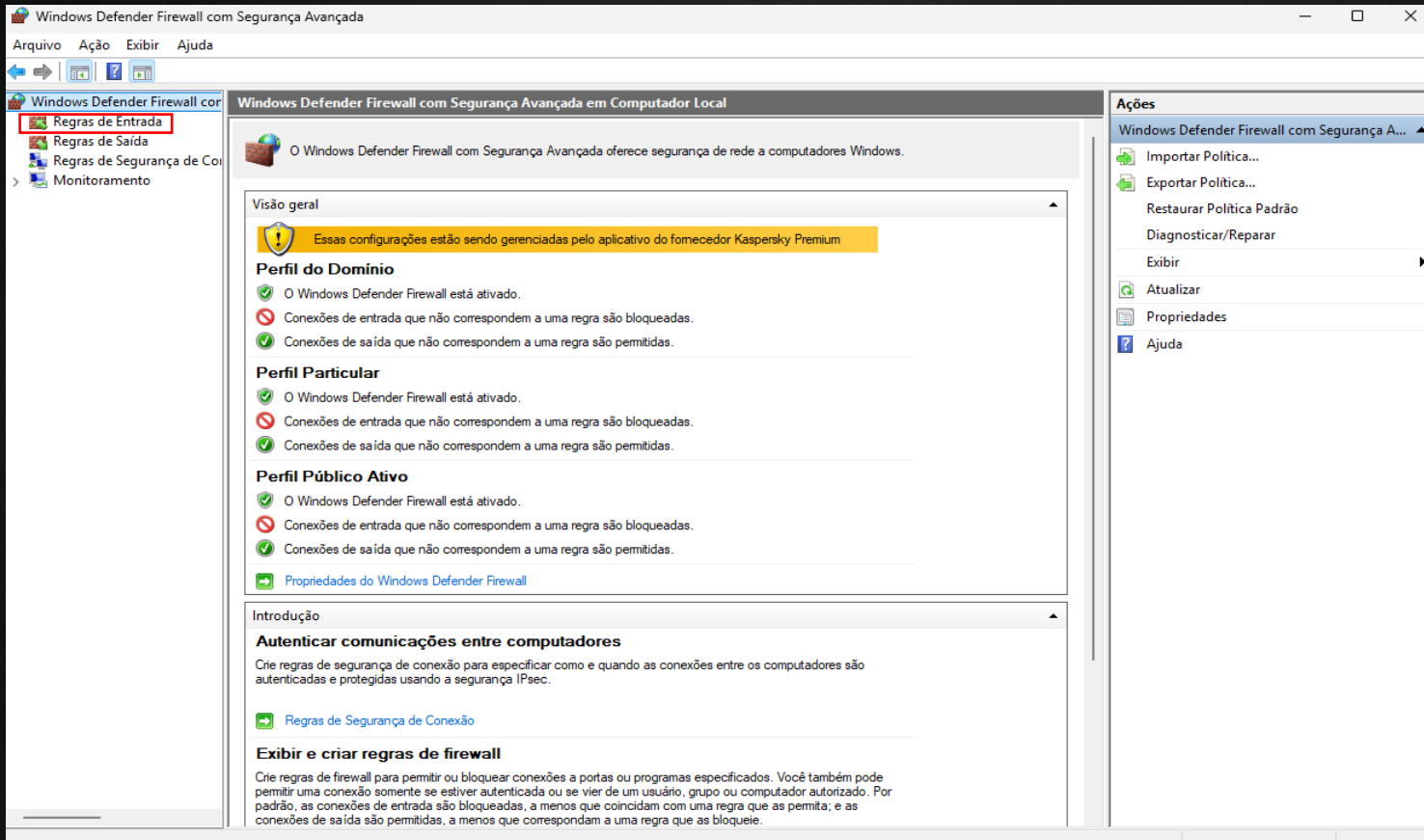

```
sudo iptables -L
```

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
sudo iptables-save > /etc/iptables/rules.v4
```

```
http://ip_do_servidor
```





The screenshot shows the Windows Defender Firewall with Advanced Security window. The left sidebar has a red box around 'Regras de Entrada'. The main pane shows the 'Visão geral' (Overview) section, which includes a warning that configurations are managed by Kaspersky Premium. Below this, three profiles are listed: 'Perfil do Domínio', 'Perfil Particular', and 'Perfil Público Ativo'. Each profile shows that the firewall is active and that incoming connections are blocked while outgoing connections are permitted. The right sidebar shows the 'Ações' (Actions) menu with options like 'Importar Política...', 'Exportar Política...', 'Restaurar Política Padrão', 'Diagnosticar/Reparar', 'Exibir', 'Atualizar', 'Propriedades', and 'Ajuda'.

Windows Defender Firewall com Segurança Avançada

Arquivo Ação Exibir Ajuda

Windows Defender Firewall com Segurança Avançada em Computador Local

O Windows Defender Firewall com Segurança Avançada oferece segurança de rede a computadores Windows.

Visão geral

Essas configurações estão sendo gerenciadas pelo aplicativo do fornecedor Kaspersky Premium

Perfil do Domínio

- ✓ O Windows Defender Firewall está ativado.
- ✗ Conexões de entrada que não correspondem a uma regra são bloqueadas.
- ✓ Conexões de saída que não correspondem a uma regra são permitidas.

Perfil Particular

- ✓ O Windows Defender Firewall está ativado.
- ✗ Conexões de entrada que não correspondem a uma regra são bloqueadas.
- ✓ Conexões de saída que não correspondem a uma regra são permitidas.

Perfil Público Ativo

- ✓ O Windows Defender Firewall está ativado.
- ✗ Conexões de entrada que não correspondem a uma regra são bloqueadas.
- ✓ Conexões de saída que não correspondem a uma regra são permitidas.

[Propriedades do Windows Defender Firewall](#)

Introdução

Autenticar comunicações entre computadores

Crie regras de segurança de conexão para especificar como e quando as conexões entre os computadores são autenticadas e protegidas usando a segurança IPsec.

[Regras de Segurança de Conexão](#)

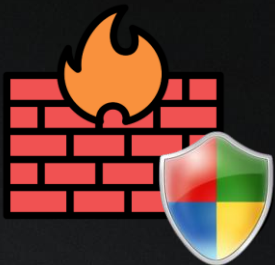
Exibir e criar regras de firewall

Crie regras de firewall para permitir ou bloquear conexões a portas ou programas especificados. Você também pode permitir uma conexão somente se estiver autenticada ou se vier de um usuário, grupo ou computador autorizado. Por padrão, as conexões de entrada são bloqueadas, a menos que coincidam com uma regra que as permita; e as conexões de saída são permitidas, a menos que correspondam a uma regra que as bloqueie.

Ações

Windows Defender Firewall com Segurança A...

- Importar Política...
- Exportar Política...
- Restaurar Política Padrão
- Diagnosticar/Reparar
- Exibir
- Atualizar
- Propriedades
- Ajuda



Windows Defender Firewall com Segurança Avançada

Arquivo Ação Exibir Ajuda

Windows Defender Firewall com Segurança Avançada

- Regras de Entrada
- Regras de Saída
- Regras de Segurança de Rede
- Monitoramento

Regras de Entrada

Nome	Grupo	Perfil	Habilitado	Ação	Substituir	Programa
4DDiG File Repair_AudioRepairService		Tudo	Sim	Permi...	Não	C:\Progra
4DDiG File Repair_MediaPlayerService		Tudo	Sim	Permi...	Não	C:\Progra
ApowerREC		Tudo	Sim	Permi...	Não	C:\Progra
BlueStacks Service		Tudo	Sim	Permi...	Não	C:\Progra
BlueStacksAppplayerWeb		Tudo	Sim	Permi...	Não	C:\Progra
BlueStacksWeb		Tudo	Sim	Permi...	Não	C:\Progra
Cloud Game		Tudo	Sim	Permi...	Não	C:\Progra
Corel PHOTO-PAINT 2020 (64-Bit)		Tudo	Sim	Bloqu...	Não	c:\Progra.
CorelDRAW 2020 (64-Bit)		Tudo	Sim	Bloqu...	Não	c:\Progra.
EEventManager.exe		Público	Sim	Permi...	Não	C:\Progra
EEventManager.exe		Público	Sim	Permi...	Não	C:\Progra
HNS Container Networking - DNS (UDP-I...		Tudo	Sim	Permi...	Não	Qualquer
HNS Container Networking - ICS DNS (T...		Tudo	Sim	Permi...	Não	%Systemf
ManyCam Virtual Webcam		Tudo	Sim	Permi...	Não	C:\Progra
Microsoft Lync		Público	Sim	Permi...	Não	C:\Progra
Microsoft Lync		Público	Sim	Permi...	Não	C:\Progra
Microsoft Lync UcMapi		Público	Sim	Permi...	Não	C:\Progra
Microsoft Lync UcMapi		Público	Sim	Permi...	Não	C:\Progra
Microsoft Office Outlook		Público	Sim	Permi...	Não	C:\Progra
Teamviewer Remote Control Application		Público	Sim	Permi...	Não	C:\Progra
Teamviewer Remote Control Application		Público	Sim	Permi...	Não	C:\Progra
Teamviewer Remote Control Service		Público	Sim	Permi...	Não	C:\Progra
Teamviewer Remote Control Service		Público	Sim	Permi...	Não	C:\Progra
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	Tudo	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domí...	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domí...	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.StartMenuExperi...	@{Microsoft.Windows.Start...	Domí...	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.StartMenuExperi...	@{Microsoft.Windows.Start...	Domí...	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.StartMenuExperi...	@{Microsoft.Windows.Start...	Domí...	Sim	Permi...	Não	Qualquer
@{Microsoft.Windows.StartMenuExperi...	@{Microsoft.Windows.Start...	Domí...	Sim	Permi...	Não	Qualquer
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domí...	Sim	Permi...	Não	Qualquer
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domí...	Sim	Permi...	Não	Qualquer
@{MicrosoftWindows.Client.Core_1000.2...	@{MicrosoftWindows.Client...	Domí...	Sim	Permi...	Não	Qualquer

Ações

- Regras de Entrada
 - Nova Regra...
 - Filtrar por Perfil
 - Filtrar por Estado
 - Filtrar por Grupo
- Exibir
 - Atualizar
 - Exportar Lista...
- Ajuda



Assistente para Nova Regra de Entrada

Tipo de regra
Selecionar o tipo de regra de firewall a ser criada.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Que tipo de regra você deseja criar?

☐ **Programa**
Regra que controla conexões para um programa.

☒ **Porta**
Regra que controla conexões para uma porta TCP ou UDP.

☐ **Predefinida:**
Assistência Remota
Regra que controla conexões para uma experiência do Windows.

☐ **Personalizado**
Regra personalizada.

< Voltar Avançar > Cancelar



Assistente para Nova Regra de Entrada

Protocolo e Portas

Especifique os protocolos e as portas a que a regra se aplica.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Essa regra se aplica a TCP ou a UDP?

☒ TCP

☐ UDP

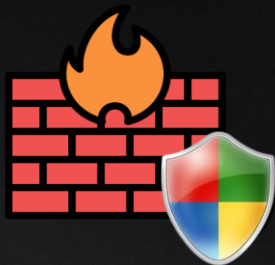
Essa regra se aplica a todas as portas locais ou a portas locais específicas?

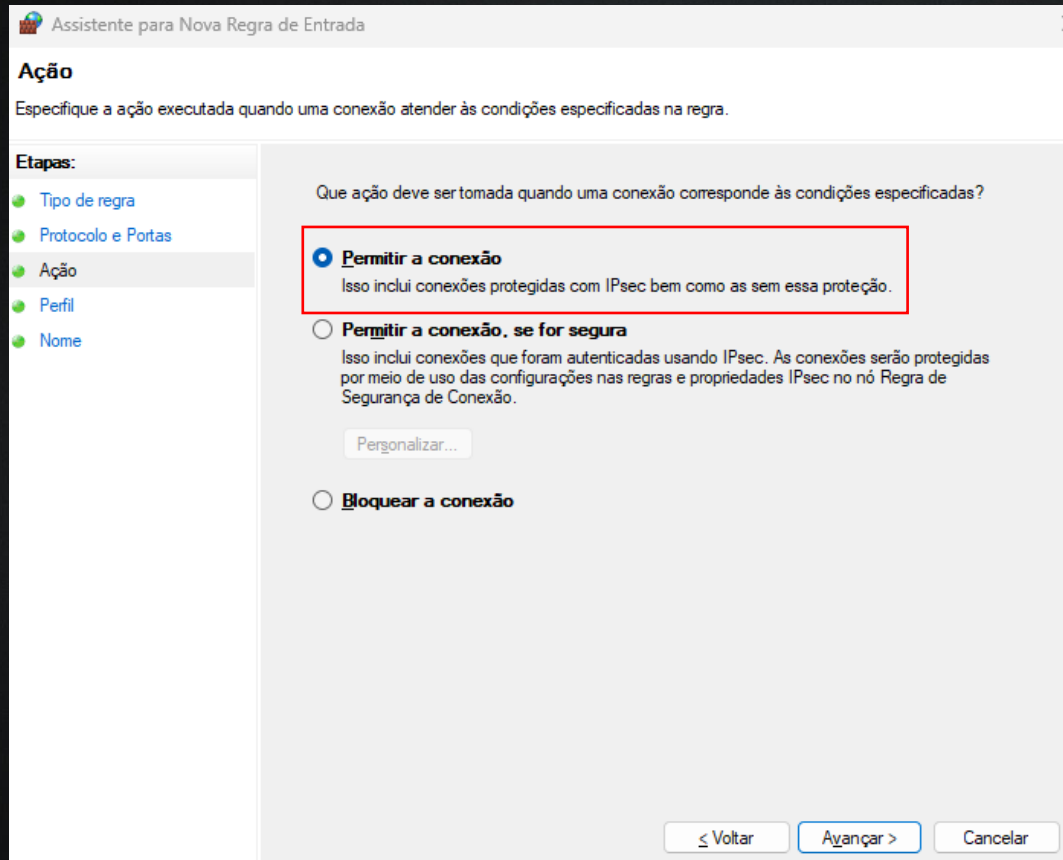
☐ Todas as portas locais

☒ Portas locais específicas:

Exemplo: 80, 443, 5000-5010

< Voltar Avançar > Cancelar





Assistente para Nova Regra de Entrada

Perfil

Especificar os perfis aos quais essa regra se aplica.

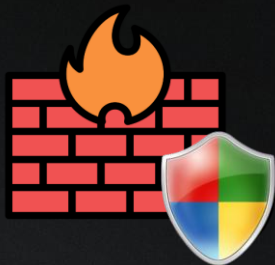
Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil**
- Nome

Quando esta regra se aplica?

- ☒ **Domínio**
Aplica-se quando um computador está conectado ao seu domínio corporativo.
- ☒ **Particular**
Aplica-se quando um computador está conectado a um local de rede privada, como residência ou local de trabalho.
- ☒ **Público**
Aplica-se quando um computador está conectado a um local de rede pública.

< Voltar Avançar > Cancelar



Assistente para Nova Regra de Entrada

Nome

Especificar o nome e a descrição desta regra.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

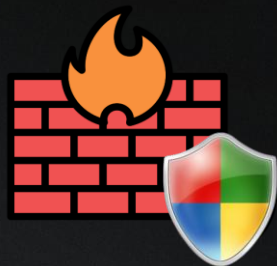
Nome:

FIAP - FIREWAL

Descrição (opcional):

Atividade de configuração de Firewall na plataforma Microsoft Widnows

< Voltar Concluir Cancelar



Assistente para Nova Regra de Entrada

Protocolo e Portas

Especifique os protocolos e as portas a que a regra se aplica.

Etapas:

- Tipo de regra
- Programa
- Protocolo e Portas**
- Escopo
- Ação
- Perfil
- Nome

A que portas e protocolos esta regra se aplica?

Tipo de protocolo: Qualquer

Número do protocolo: 0

Porta local: Todas as Portas

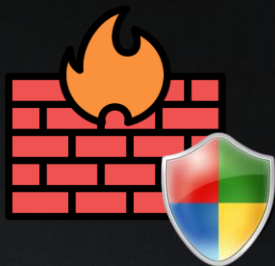
Exemplo: 80, 443, 5000-5010

Porta remota: Todas as Portas

Exemplo: 80, 443, 5000-5010

Configurações ICMP: Personalizar...

< Voltar Avançar > Cancelar



Assistente para Nova Regra de Entrada

Escopo

Especifique os endereços IP local e remoto correspondentes a esta regra.

Etapas:

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo**
- Ação
- Perfil
- Nome

A quais endereços IP locais esta regra se aplica?

☒ Qualquer endereço IP

☐ Estes endereços IP:

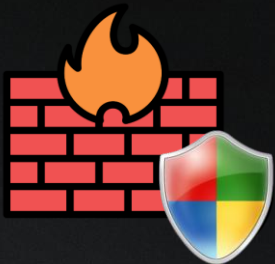
Personalizar os tipos de interface aos quais esta regra se aplica:


A quais endereços IP remotos esta regra se aplica?

☒ Qualquer endereço IP

☐ Estes endereços IP:

< Voltar Avançar > Cancelar



 Assistente para Nova Regra de Entrada

Ação

Especifique a ação executada quando uma conexão atender às condições especificadas na regra.

Etapas:

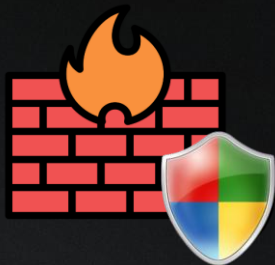
- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- Ação
- Perfil
- Nome

Que ação deve ser tomada quando uma conexão corresponde às condições especificadas?

☐ Permitir a conexão
Isso inclui conexões protegidas com IPsec bem como as sem essa proteção.

☐ Permitir a conexão, se for segura
Isso inclui conexões que foram autenticadas usando IPsec. As conexões serão protegidas por meio de uso das configurações nas regras e propriedades IPsec no nó Regra de Segurança de Conexão.

☒ Bloquear a conexão



Assistente para Nova Regra de Entrada

Perfil

Especificar os perfis aos quais essa regra se aplica.

Etapas:

- Tipo de regra
- Programa
- Protocolo e Portas
- Escopo
- Ação
- Perfil**
- Nome

Quando esta regra se aplica?

- ☒ **Domínio**
Aplica-se quando um computador está conectado ao seu domínio corporativo.
- ☒ **Particular**
Aplica-se quando um computador está conectado a um local de rede privada, como residência ou local de trabalho.
- ☒ **Público**
Aplica-se quando um computador está conectado a um local de rede pública.

[< Voltar](#) [Avançar >](#) [Cancelar](#)



Assistente para Nova Regra de Entrada

Nome

Especificar o nome e a descrição desta regra.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Nome:

FIAP - FIREWAL

Descrição (opcional):

Atividade de configuração de Firewall na plataforma Microsoft Widnows

< Voltar Concluir Cancelar



Até a Próxima...