

Fundamentos de Segurança Cibernética



Conceitos e Aplicações Práticas

Prof. Ronierison Maciel

27/11/2023

O que veremos hoje?

- Conceitos introdutórios de segurança da informação.

Introdução

- Quantidade de informações produzida a cada dia
- O sistema da minha empresa é seguro?
- Será que isso acontecerá na minha empresa?
- Como minimizar os riscos?



Introdução

E quanto às suas informações pessoais, você se preocupa com a sua segurança?



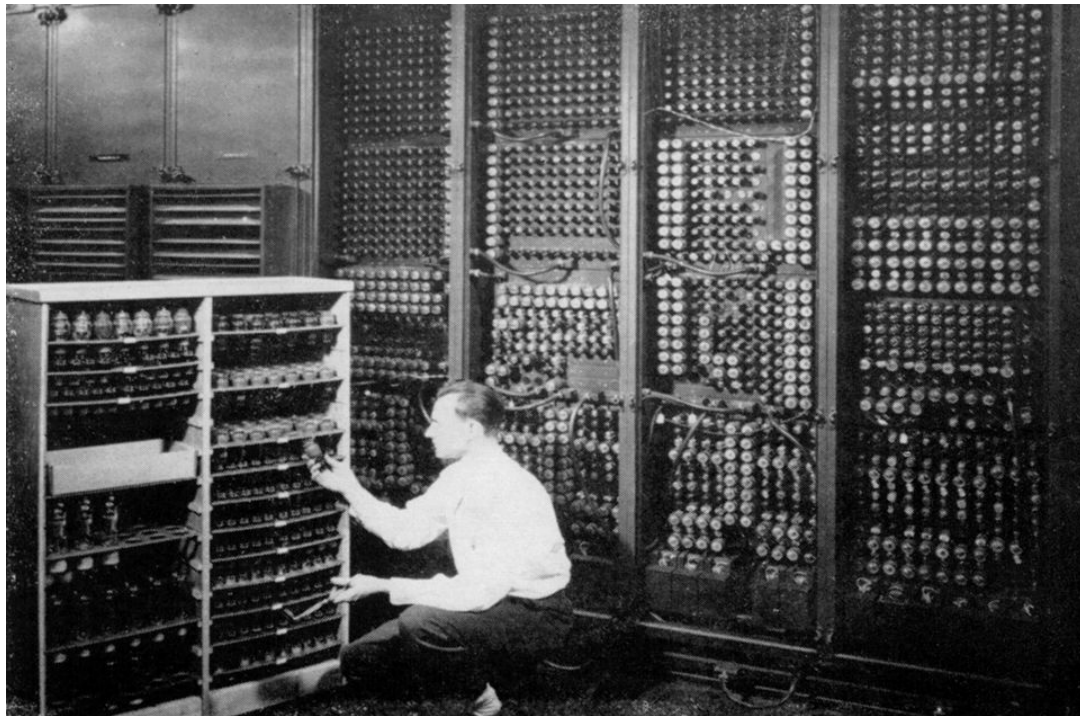
Introdução

O que torna um sistema seguro?



Introdução

Antigamente



Introdução

Atualmente



Introdução

Ameaças



Introdução

Informação: O bem mais valioso



Introdução

Vamos aos conceitos básicos da área de
segurança da informação....

Introdução

A tríade da segurança da informação.



Confidencialidade

Proteção contra acesso não autorizado a dados.



Integridade

Proteção contra alteração dos dados.



Disponibilidade

Proteção contra a interrupção de acesso aos dados e ou serviços.



Segurança


Os 5 aspectos adicionais da segurança da
informação

Segurança da Informação





Autenticação

Garantir que um usuário é de fato quem ele alega ser.



SIGN IN

 USERNAME

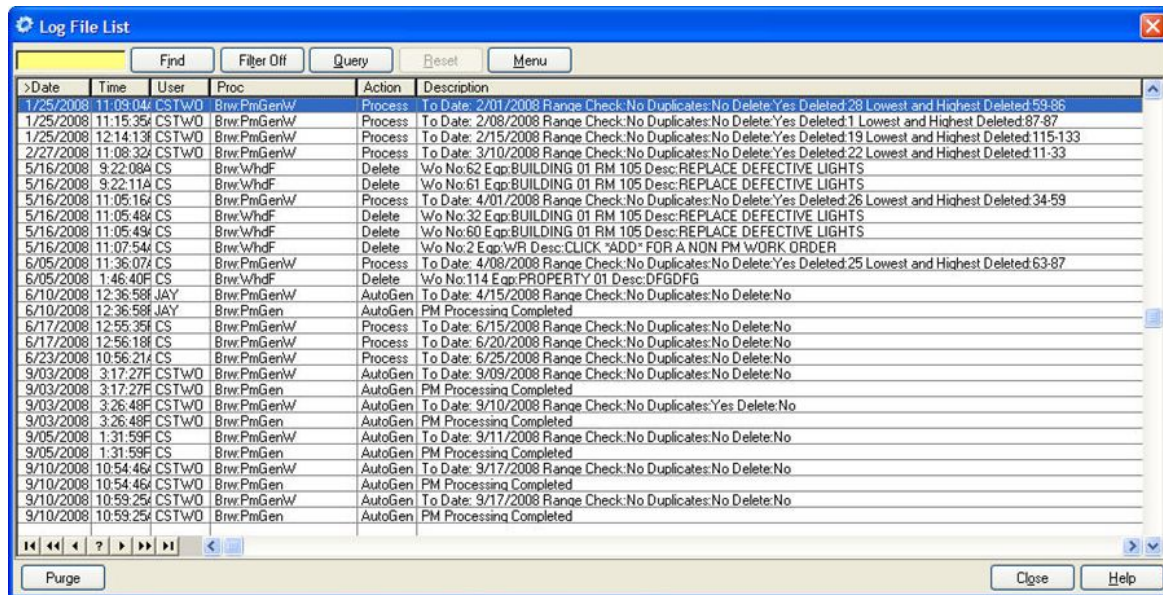
 PASSWORD

LOGIN

☒ Remember Me [Forgot Password?](#)

Não-repúdio

Capacidade do sistema “**provar**” que o usuário executou determinada ação.



The screenshot shows a window titled "Log File List" with a table of log entries. The table has columns for Date, Time, User, Proc, Action, and Description. The logs show various system processes and user actions, including range checks, deletions, and property updates, with specific dates and times recorded for each entry.

Date	Time	User	Proc	Action	Description
1/25/2008	11:09:04	CSTW0	BrrwPmGenW	Process	To Date: 2/01/2008 Range Check:No Duplicates:No Delete:Yes Deleted:28 Lowest and Highest Deleted:59-86
1/25/2008	11:15:35	CSTW0	BrrwPmGenW	Process	To Date: 2/08/2008 Range Check:No Duplicates:No Delete:Yes Deleted:1 Lowest and Highest Deleted:87-87
1/25/2008	12:14:13	CSTW0	BrrwPmGenW	Process	To Date: 2/15/2008 Range Check:No Duplicates:No Delete:Yes Deleted:19 Lowest and Highest Deleted:115-133
2/27/2008	11:08:32	CSTW0	BrrwPmGenW	Process	To Date: 3/10/2008 Range Check:No Duplicates:No Delete:Yes Deleted:22 Lowest and Highest Deleted:11-33
5/16/2008	9:22:08	CS	BrrwW/hdF	Delete	W/o No:62 Eqp:BUILDING 01 RM 105 Desc:REPLACE DEFECTIVE LIGHTS
5/16/2008	9:22:11	CS	BrrwW/hdF	Delete	W/o No:61 Eqp:BUILDING 01 RM 105 Desc:REPLACE DEFECTIVE LIGHTS
5/16/2008	11:05:16	CS	BrrwPmGenW	Process	To Date: 4/01/2008 Range Check:No Duplicates:No Delete:Yes Deleted:26 Lowest and Highest Deleted:34-59
5/16/2008	11:05:49	CS	BrrwW/hdF	Delete	W/o No:32 Eqp:BUILDING 01 RM 105 Desc:REPLACE DEFECTIVE LIGHTS
5/16/2008	11:05:49	CS	BrrwW/hdF	Delete	W/o No:60 Eqp:BUILDING 01 RM 105 Desc:REPLACE DEFECTIVE LIGHTS
5/16/2008	11:07:54	CS	BrrwW/hdF	Delete	W/o No:2 Eqp:W/R Desc:CLICK "ADD" FOR A NON PM WORK ORDER
6/05/2008	11:36:07	CS	BrrwPmGenW	Process	To Date: 4/08/2008 Range Check:No Duplicates:No Delete:Yes Deleted:25 Lowest and Highest Deleted:63-87
6/05/2008	1:46:40	CS	BrrwW/hdF	Delete	W/o No:114 Eqp:PROPERTY 01 Desc:DFGDFG
6/10/2008	12:36:58	JAY	BrrwPmGenW	AutoGen	To Date: 4/15/2008 Range Check:No Duplicates:No Delete:No
6/10/2008	12:36:58	JAY	BrrwPmGen	AutoGen	PM Processing Completed
6/17/2008	12:55:35	CS	BrrwPmGenW	Process	To Date: 6/15/2008 Range Check:No Duplicates:No Delete:No
6/17/2008	12:56:18	CS	BrrwPmGenW	Process	To Date: 6/20/2008 Range Check:No Duplicates:No Delete:No
6/23/2008	10:56:21	CS	BrrwPmGenW	Process	To Date: 6/25/2008 Range Check:No Duplicates:No Delete:No
9/03/2008	3:17:27	CSTW0	BrrwPmGenW	AutoGen	To Date: 9/09/2008 Range Check:No Duplicates:No Delete:No
9/03/2008	3:17:27	CSTW0	BrrwPmGen	AutoGen	PM Processing Completed
9/03/2008	3:26:48	CSTW0	BrrwPmGenW	AutoGen	To Date: 9/10/2008 Range Check:No Duplicates:Yes Delete:No
9/03/2008	3:26:48	CSTW0	BrrwPmGen	AutoGen	PM Processing Completed
9/05/2008	1:31:59	CS	BrrwPmGenW	AutoGen	To Date: 9/11/2008 Range Check:No Duplicates:No Delete:No
9/05/2008	1:31:59	CS	BrrwPmGen	AutoGen	PM Processing Completed
9/10/2008	10:54:46	CSTW0	BrrwPmGenW	AutoGen	To Date: 9/17/2008 Range Check:No Duplicates:No Delete:No
9/10/2008	10:54:46	CSTW0	BrrwPmGen	AutoGen	PM Processing Completed
9/10/2008	10:59:25	CSTW0	BrrwPmGenW	AutoGen	To Date: 9/17/2008 Range Check:No Duplicates:No Delete:No
9/10/2008	10:59:25	CSTW0	BrrwPmGen	AutoGen	PM Processing Completed

Legalidade

O uso da tecnologia de informática e comunicação deve seguir as leis local ou país.

O que é a Lei Carolina Dieckmann?

- Apelidada de Lei Carolina Dieckmann, a **Lei dos Crimes Cibernéticos (12.737/2012)** tipifica como crimes infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou "derrubar" sites. O projeto foi elaborado na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e espalhadas pela rede mundial de computadores.

Privacidade

Capacidade de um sistema manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações.



Auditoria

Uma auditoria em Segurança da Informação é uma avaliação sistemática da segurança do sistema de informação de uma empresa. Basicamente, ela busca medir o quanto o sistema está em conformidade com um conjunto de critérios estabelecidos



Segurança

Não-repúdio

Provar **QUEM** fez

O QUE e **ONDE**

Para um **usuário** em
específico

Auditoria

Ir em busca de fraudes

Para todo o **sistema**

Então



Incidente de segurança

É a ocorrência de um evento que possa causar **interrupções** nos **processos** em consequência da violação de algum dos aspectos listados acima.

Outros fatores são secundários

- Intempéries da natureza;
- Greves;
- Manifestações.



Quem é quem...

Um agente externo pode oferecer uma **ameaça** a um sistema que encontra-se em estado de **vulnerabilidade** podendo efetuar um **ataque**. Por isso é importante haver um **controle** sobre as vulnerabilidades para minimizar a **probabilidade** de chance de falha e **impactos** indesejados.

Ameaça

Um agente externo que oferece perigo.



Vulnerabilidade

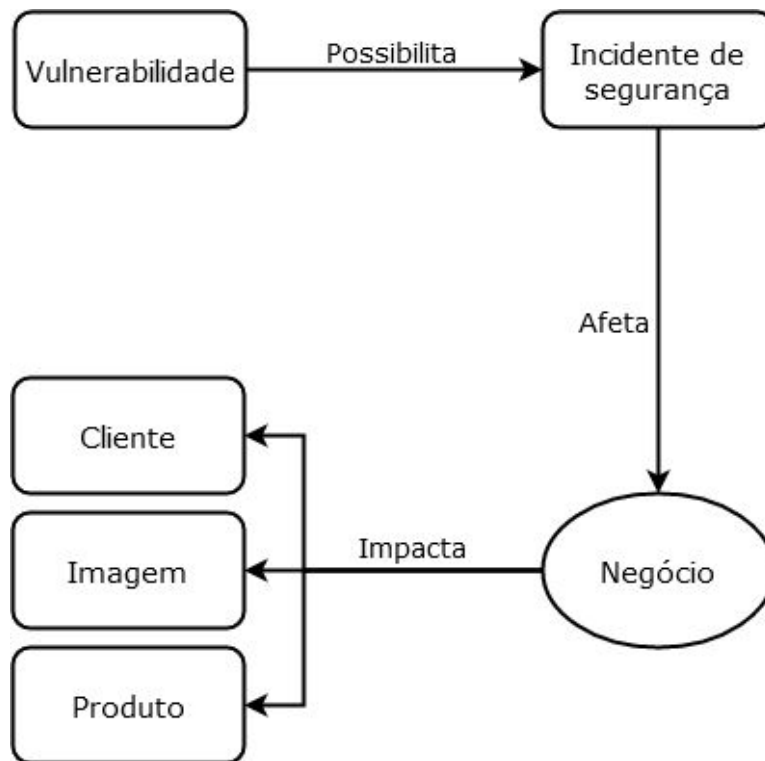
É uma **fraqueza** que **permite** que um **atacante** reduza a garantia da informação de um sistema.



Vulnerabilidades

- Físicas;
- Naturais;
- Hardware;
- Software;
- Mídias;
- Comunicação;
- Humanas.

Fluxograma da vulnerabilidade



Ataque

Agente externo em ação busca obter algum tipo de retorno atingindo algum ativo de valor.

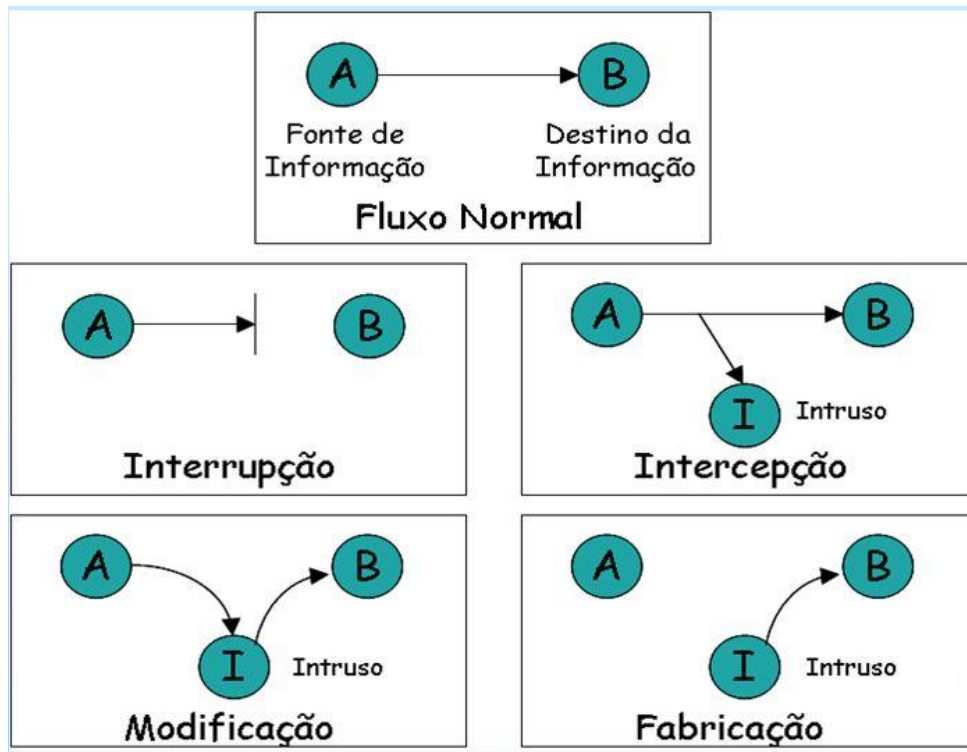


Tipos de ataques

Um ataque pode ser:

1. **Ativo** - tendo por resultado a alteração dos dados;
2. **Passivo** - tendo por resultado a liberação dos dados,
Por exemplo: sequestro de URL, phishing e outros ataques baseados em engenharia social;
3. **Destrutivo** - visando à negação do acesso aos dados ou serviços.

Mecanismos de ataques



Definição

- Controle
 - Prevenção contra ataques combatendo as vulnerabilidades.
- Probabilidade
 - É possível medir tanto a vulnerabilidade quanto ameaças!

Definição

- Impactos
 - O impacto de um incidente de segurança é medido pelas consequências que possa causar aos processos de negócio suportados pelo ativo em questão.

Tipos de impactos

- **OPERACIONAL**

- Interrupções ou indisponibilidade de processos;

- **FINANCEIRA**

- Lucro cessante, penalidade contratuais ou legais e outros;

- **IMAGEM**

- Desgaste da imagem da organização junto a força de trabalho (valores) e/ou ao mercado (clientes...)

O que veremos hoje?

- A Segurança e o ciclo de vida da informação
- Classificação e controle dos ativos de informação
- Discussão sobre o tema no final da aula

Introdução

A segurança e o ciclo de vida da informação

Fluxo

1. Identificação
2. Obtenção
3. Tratamento
4. Distribuição
5. Uso
6. Armazenamento
7. Descarte

Identificação

- Identificação das necessidades e dos requisitos (1/7)



Obtenção

- Obtenção das informações, onde se faz necessária a repetição contínua de alimentação do processo (2/7)



Tratamento

- Antes de estar em condições de ser aproveitada, é comum a informação precisa passar por processos [...] com o propósito de torná-la mais acessível e fácil de localizar pelos usuários (3/7)



Distribuição

- Significa dizer que a informação será conduzida ao usuário que dela necessita (4/7)



Diretora

Vice-diretor

Conselheiro acadêmico

Conselheiro acadêmico

Moderadores

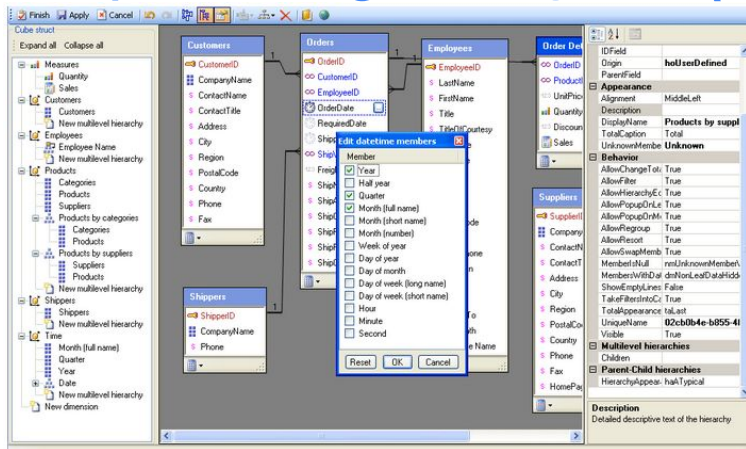
Professores

Demais funcionários

Alunos monitores

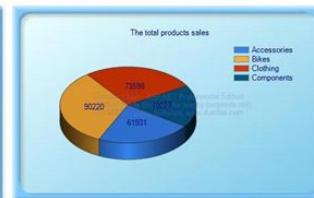
Alunos

- Mais importante de todo o processo de gestão da informação, embora seja frequentemente ignorada pelas organizações (5/7)



OLAP grid

Fiscal Year		FY 2002				Total	
Measures	Order Quantity	Value	Goal	Status	Trend	Order Quantity	Product Gross Profit
Accessories	1 825	40,38%	40,00%	0,00%		1 825	40,38%
Bikes	4 951	4,84%	12,00%	0,00%		4 951	4,84%
Components	10 331	18,38%	12,00%	0,00%		10 331	18,38%
Total	15 282	12,31%	12,00%	0,00%		15 282	12,31%



Armazenamento

- É a conservação dos dados e informações, permitindo seu uso e reuso dentro da organização (6/7)



Descarte

- Significa dizer, que se uma informação se torna obsoleta ou inútil ela deve ser rejeitada (7/7)



Introdução

Classificação e controle dos ativos de informação

O que é a classificação?

Qual a informação mais importante?



Ativos da informação

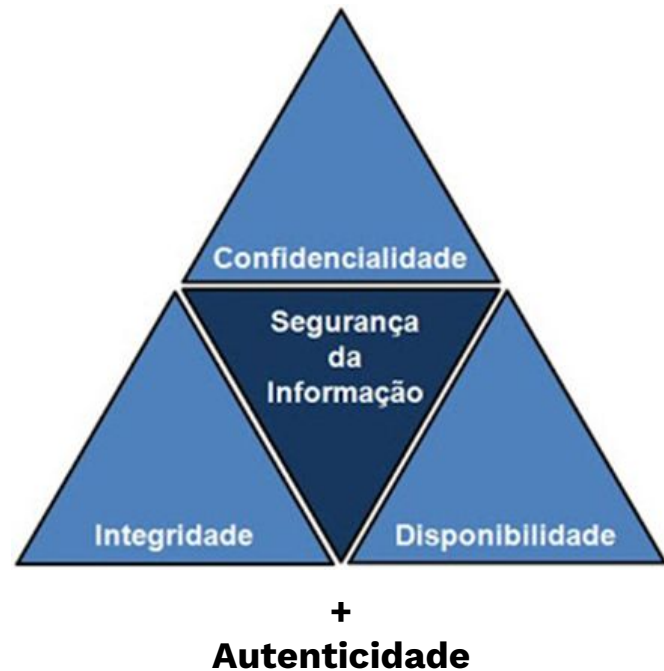
- Software
- Físico
- Serviços
- Pessoas
- Documento em Papel
- Informação

Como classificar?

- Primeiro, alguns conceitos importantes
 - **Classificação:** atividade de atribuir o grau de sigilo a um ativo da informação
 - **Proprietário:** responsável pelo ativo da informação.
 - **Custodiante:** responsável pela guarda do ativo da informação.

O que deve-se considerar?

- Devemos considerar:



Como classificar?

- Formas de Classificação, quanto a:
 1. Confidencialidade
 2. Disponibilidade
 3. Integridade
 4. Autenticidade
 5. Monitoramento Contínuo.

Confidencialidade

1. Nível

1.1. Informação Pública

2. Nível

2.1. Informação Interna

3. Nível

3.1. Informação Confidencial

4. Nível

4.1. Informação Secreta

Confidencialidade

1. Informação Pública



Confidencialidade

2. Informação Interna



Confidencialidade

3. Informação Confidencial

1	123456	17	michael
2	12345	18	ashley
3	123456789	19	654321
4	password	20	qwerty
5	iloveyou	21	iloveu
6	princess	22	michelle
7	rockyou	23	111111
8	1234567	24	0
9	12345678	25	tigger
10	abc123	26	password1
11	nicole	27	sunshine
12	daniel	28	chocolate
13	babygirl	29	anthony
14	monkey	30	angel
15	jessica	31	FRIENDS
16	lovely	32	soccer

Confidencialidade

4. Informação Secreta



Confidencialidade

Outra classificação a nível de informações do setor público.



Decreto 4.553/2002

Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, bem como das áreas e instalações onde tramitam.

Revogado pelo 7.845/2012

Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Ultra-secretos

A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público **autorizado**, ou transmitidas por meio **eletrônico**, desde que sejam usados recursos de **criptografia compatíveis** com o **grau de classificação da informação**, vedada sua postagem.

Classificação

Como fazer a classificação?

Qual a falta que a informação faz?

Disponibilidade

- Classificação quanto à disponibilidade
 - **Nível 1** - Informações devem ser recuperadas em minutos
 - **Nível 2** - ... horas
 - **Nível 3** - ... dias
 - **Nível 4** - ... não críticas



Integridade

- Classificação quanto à integridade
 - Está de acordo com a **especificação?**



Autenticidade

- Classificação quanto à Autenticidade
 - É realmente **autenticavel**?



Monitoramento contínuo

- Depois da classificação deve-se manter o processo de reclassificação contínua.

Debate

- É possível espionar o nosso país?
 - se sim, como?
- O quanto nossa “infraestrutura”. É segura!?
 - se sim, porquê?
- Quais as últimas vulnerabilidades expostas?
 - cite pelo menos 3 vulnerabilidades.



O que veremos hoje?

- Avaliação do conhecimento adquirido até aqui.
- Assunto de Hoje: **Aspectos Humanos na Segurança da Informação**

Introdução

Aspectos Humanos na Segurança da Informação

O que as pessoas são capazes?



Chief Security Officer



x



Chief Security Officer

- **Atividades**

- **Coordenação** da área de segurança e da infra-estrutura organizacional;
- **Planejamento** dos investimentos de segurança;
- **Definição** dos índices e indicadores para a segurança;
- **Definição**, elaboração, divulgação, treinamento, implementação, e administração da política de segurança etc;
- **Análise** de riscos envolvendo segurança;
- **Investigação** sobre incidentes de segurança.

Engenharia Social



Engenharia Social

- Segundo o SANS Institute:
 - *“Engenharia Social é a arte de utilizar o comportamento humano para quebrar a segurança sem que a vítima sequer perceba que foi manipulada”*

Engenharia Social

- Segundo CERT.Br:

- *“É um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado aos ativos da informação”*

Engenharia Social

- Pode ser estudada sob as perspectivas **FÍSICAS** e **PSICOLÓGICAS**

Engenharia Social (Físicas)




DARUMA DEVELOPERS COMMUNITY

Suporte ao Desenvolvedor
 Daruma Developer Community
 Ligação Gratuita
 0800 770 3320

CNPJ: 45.170.289/0001-25
 IE: 688023460111
 IM: 363372
 04/07/2012 14:21:08 CCF:002707 C00:003478

CUPOM FISCAL
 ITEM CODIGO DESCRICAO QTD UN VL UNIT 8% ST A/T VL ITEM 8%
 001 54230301146 Bloco de notas 1UN 11 2,20)

TOTAL R\$ 2,20
 Dinheiro 2,20

CNPJ/CPF Consumidor: 123.123.123-99
 NOME: Benedito Frôscolo Jovino
 ENDEREÇO: Av. Paulista, 2911 - São Paulo

207 E96B4 389FD F09030 03 BIL203 B5C7F 1921F 614
 DARUMA AUTOMAÇÃO FS700 H
 ECF-IF VERSÃO:01.01.00 ECF:001 LJ:004
 888888888888F16FDIO 04/07/2012 14:21:56
 FAB:DR0509BR00C0000181273 *BR*

Engenharia Social (Físicas)



Engenharia Social (Psicológicas)

Ingenuidade



Por que cuidar da segurança?

Usuários que **NÃO** dominam computadores

Usuários que **dominam** computadores

Administradores

Contrato de trabalho

- Termo de Confidencialidade



Seleção pessoal



Treinamento pessoal



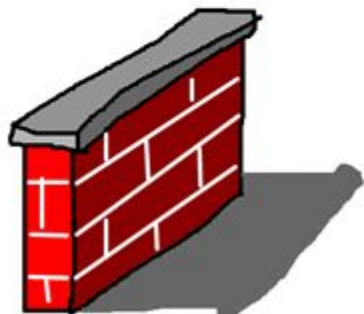
O que veremos hoje?

- Segurança em ambientes Físicos e Lógicos

Tipos de Barreiras de Segurança

- ISO 17799

Física



Lógica

A screenshot of a web-based sign-in form. It includes a 'Sign in' header, a 'Google' logo, and input fields for 'Username' and 'Password'. Below the fields are a blue 'Sign in' button, a checkbox for 'Stay signed in', and a link for 'Can't access your account?'. The form is set against a light grey background.

ISO 27000

- Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

Dicas

- Siglas

- **ABNT** = Associação Brasileira de Normas Técnicas
- **NBR** = Normas BRasileiras
- **ISO** = International Organization for Standardization
(Organização Internacional de Normalização ou Organização Internacional para Padronização)
- **IEC** = International Electrotechnical Commission (Comissão Eletrotécnica Internacional)

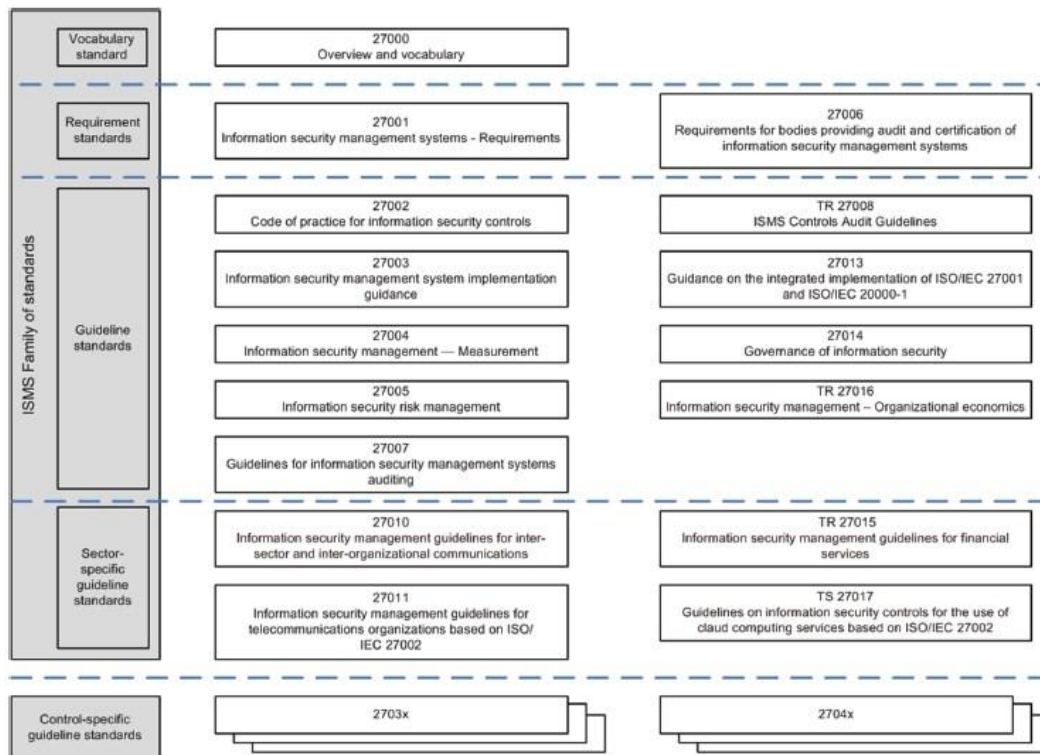
ISO 27000

- A família ISO 27000 - Sistema de Gerenciamento de Segurança:
 - ISO/IEC 27000:2009 - Sistema de Gerenciamento de Segurança-Explicação Série de normas, objetivos e vocabulários;
 - ISO/IEC 27002:2013 - Código de Melhores Práticas para a Gestão de Segurança da Informação-Mostra o caminho de como alcançar os controles certificados na ISO 27001. Essa ISO é certificável para profissionais e não para empresas;

ISO 27000

- ISO/IEC 27001:2013- Sistema de Gestão de Segurança da Informação. Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

ISO 27000



Segurança

Segurança em ambiente FÍSICO

Perímetro de Segurança



Segurança

- Segurança do ambiente de trabalho
 - Contra o quê?



Segurança

- Treinamento a quem adentra áreas comuns



Segurança

- Segurança de equipamentos



Segurança

- Segurança de documentos (em papel)
 - Cuidados
 - Uso de rótulos
 - Política de armazenamento
 - Procedimentos para manipulação
- Atenção a papéis sensíveis!

Segurança

- Segurança de documentos (eletrônicos)
 - **Possui outras questões**
 - Aparato tecnológico para visualização
 - Integridade das informações
- **Atenção à obsolescência tecnológica.**
 - **Ex. disquetes não são mais utilizados!**

Segurança

- **Segurança no cabeamento (elétrico e telecomunicações)**
 - Sempre que possível usar linhas subterrâneas
 - Proteção contra interceptações
 - Separação de cabos elétricos e de comunicação
 - Condutores blindados

Vídeo exemplo

- Data Center Locaweb



Vídeo exemplo

- Data Center Google



Vídeo exemplo

- Google Data Center Security



Segurança

Segurança em ambiente LÓGICO

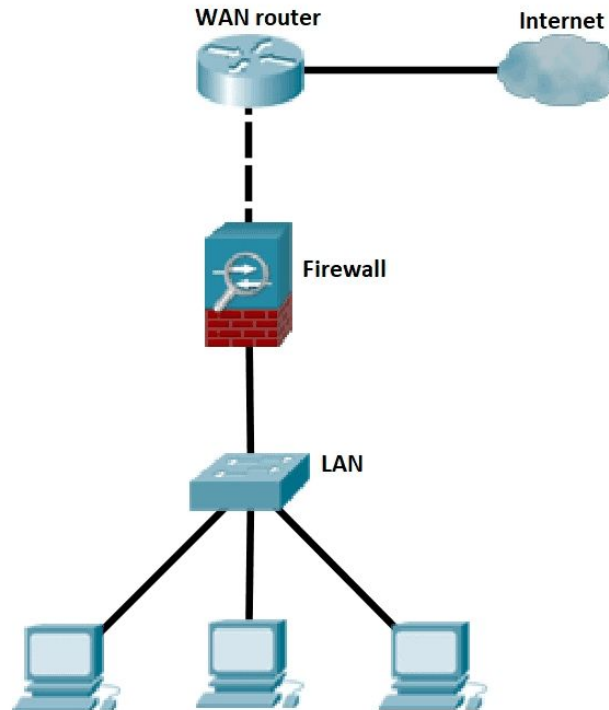


Segurança em redes

- Que mecanismos devemos utilizar?



Conceito de Firewalls e (IDS)



Introdução

→ Firewalls:

- ◆ Estes são dispositivos ou programas de software projetados para proteger redes de computadores contra acessos não autorizados. Eles atuam como uma barreira, filtrando o tráfego de rede com base em um conjunto de regras de segurança.

→ Sistemas de Detecção de Intrusos (IDS):

- ◆ São sistemas que monitoram o tráfego de rede para identificar atividades suspeitas ou maliciosas. Eles funcionam como uma medida de vigilância, alertando os administradores de rede sobre possíveis violações de segurança.

Tipos de firewalls e IDS

→ Stateful Firewalls:

- ◆ Estes firewalls acompanham o estado das sessões de rede ativas e tomam decisões de filtragem com base no contexto dessa sessão. Eles são mais sofisticados e oferecem maior segurança.

→ Stateless Firewalls:

- ◆ Trabalham filtrando pacotes individuais com base em regras pré-definidas, sem considerar o estado da conexão. São mais simples e rápidos, mas menos seguros em comparação aos stateful.

Tipos de firewalls e IDS

→ Baseado em Assinatura:

- ◆ Estes IDS detectam atividades maliciosas comparando o tráfego de rede com um banco de dados de assinaturas de ameaças conhecidas. Eles são eficazes contra ameaças conhecidas, mas podem não detectar novas variantes ou ataques zero-day.

→ Baseado em Anomalia:

- ◆ Este tipo de IDS identifica atividades suspeitas ao analisar desvios em relação ao comportamento normal da rede. Eles são úteis para detectar novas ameaças, mas podem gerar falsos positivos

Fundamentos de Firewalls e IDS

→ Conceitos Básicos:

- ◆ Explicações detalhadas sobre o que são firewalls e IDS, incluindo suas funções e importância na segurança de redes.

→ Políticas de Segurança:

- ◆ Discussão sobre a importância de estabelecer políticas claras de segurança para guiar as configurações do firewall e do IDS.

Tipos Avançados de Firewalls e IDS

→ Firewalls Avançados:

- ◆ Abordagem sobre firewalls de próxima geração (NGFW), que integram funcionalidades adicionais como inspeção profunda de pacotes e prevenção de intrusões.

→ IDS Avançados:

- ◆ Discussão sobre sistemas de prevenção de intrusões (IPS) e a diferença entre IDS e IPS.

Configuração e Implementação

→ Configuração de Firewalls:

- ◆ Instruções passo a passo sobre como configurar diferentes tipos de firewalls, incluindo regras de filtragem e políticas de segurança.

→ Instalação de IDS:

- ◆ Orientações sobre como instalar e configurar sistemas de detecção de intrusos, com foco em customização para diferentes ambientes de rede.

Monitoramento e Manutenção

→ Gerenciamento de Firewalls:

- ◆ Dicas sobre como monitorar e manter firewalls, incluindo atualizações e ajustes de políticas.

→ Análise de Dados do IDS:

- ◆ Ensina como analisar os alertas gerados pelos sistemas de detecção de intrusos e como responder a incidentes de segurança.

→ Aplicações Práticas:

- ◆ Exemplos reais e estudos de caso mostrando como firewalls e IDS são utilizados em ambientes corporativos e desafios comuns enfrentados.

Vamos praticar!



IPTables

O IPTables é uma ferramenta de filtragem de pacotes, essencialmente um firewall, utilizada em sistemas operacionais baseados em Linux. Sua principal função é **controlar** o **tráfego** de entrada, saída e encaminhamento de dados em um sistema de computador. O **IPTables** trabalha **examinando** os **pacotes** de **dados** que passam pela rede e decidindo o que fazer com eles com base em um conjunto de regras definidas pelo usuário.

IPTables - Regras

As regras determinam como o **IPTables** deve **tratar** diferentes tipos de **tráfego** de **rede**. Por exemplo, podem ser configuradas regras para **bloquear tráfego** de certos endereços IP, permitir conexões em portas específicas ou proteger o sistema contra ataques comuns de rede. O **IPTables** é **extremamente flexível** e pode ser configurado para atender a uma ampla gama de necessidades de segurança de rede, tornando-o uma ferramenta valiosa para administradores de sistemas e profissionais de segurança de TI.

IPTables - Resumo

→ Filtrar Tráfego:

- ◆ Controlar quais pacotes de dados podem entrar, sair ou passar pelo sistema.

→ Segurança de Rede:

- ◆ Proteger o sistema contra acessos não autorizados ou maliciosos.

→ Gerenciamento de Tráfego:

- ◆ Definir regras específicas para como diferentes tipos de tráfego de rede são tratados.

Passo a passo

→ Instalar ou Atualizar o IPTables:

- ◆ Execute: `$ sudo apt-get install iptables`

→ Entender as Cadeias (Chains):

- ◆ **INPUT:** Controla pacotes de entrada.
- ◆ **FORWARD:** Filtra pacotes de entrada sendo encaminhados.
- ◆ **OUTPUT:** Gerencia pacotes e conexões de saída.

→ Verificar Comportamento Padrão:

- ◆ Execute: `$ sudo iptables -L`

Passo a passo

→ Definir Política Padrão para Aceitar Conexões:

- ◆ `$ sudo iptables --policy INPUT ACCEPT`
- ◆ `$ sudo iptables --policy OUTPUT ACCEPT`
- ◆ `$ sudo iptables --policy FORWARD ACCEPT`

→ Configurar Regras Específicas para Conexões:

- ◆ Opções: **ACEITAR**, **DESCARTAR** “(DROP)”, **REJEITAR**.
- ◆ Para bloquear um IP específico: `$ sudo iptables -A INPUT -S [IP] -j DROP`

Passo a passo

→ Regras para Comunicação Bidirecional (exemplo com SSH):

◆ Permitir conexões SSH:

- `$ sudo iptables -A INPUT -p tcp --dport ssh -s [IP] -m state --state NEW,ESTABLISHED -j ACCEPT`
- `$ sudo iptables -A OUTPUT -p tcp --sport 22 -d [IP] -m state --state ESTABLISHED -j ACCEPT`

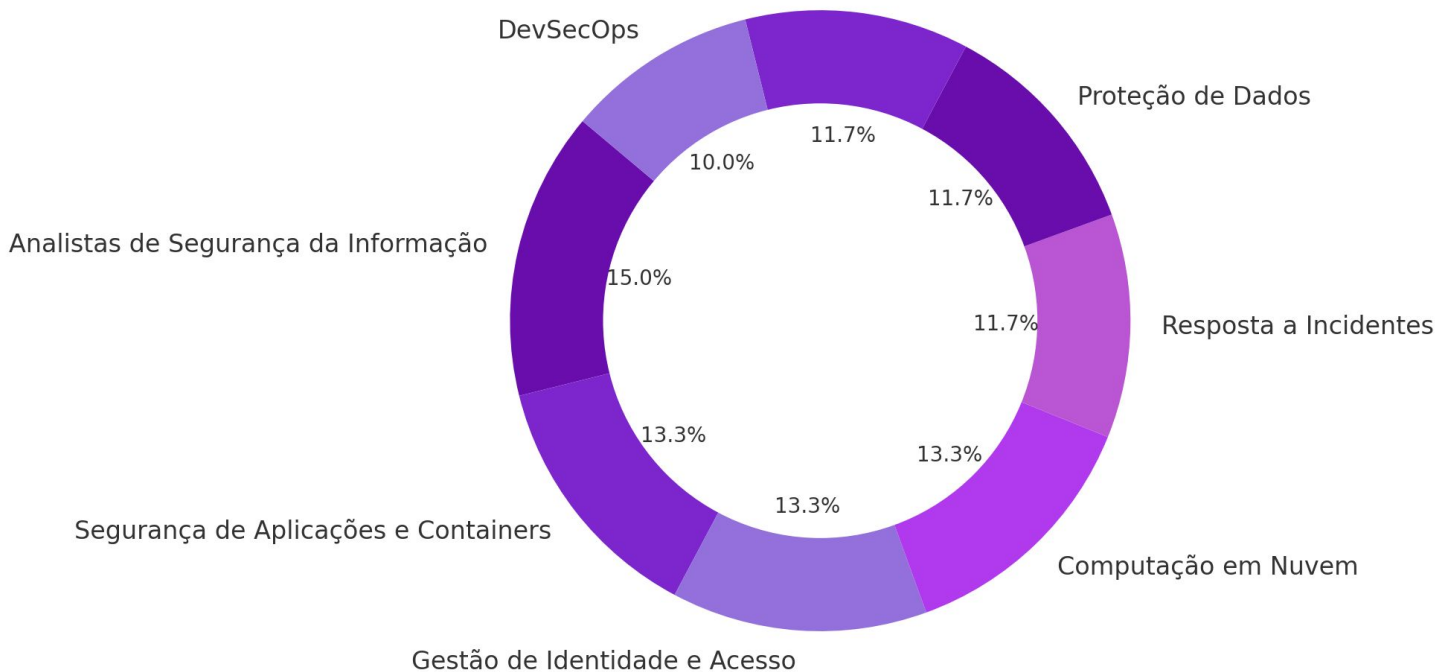
Passo a passo

→ Excluir Regras:

- ◆ Para excluir uma regra específica: `$ sudo iptables -D INPUT [número da regra]`.
- ◆ Para limpar todas as regras: `$ sudo iptables -F`.

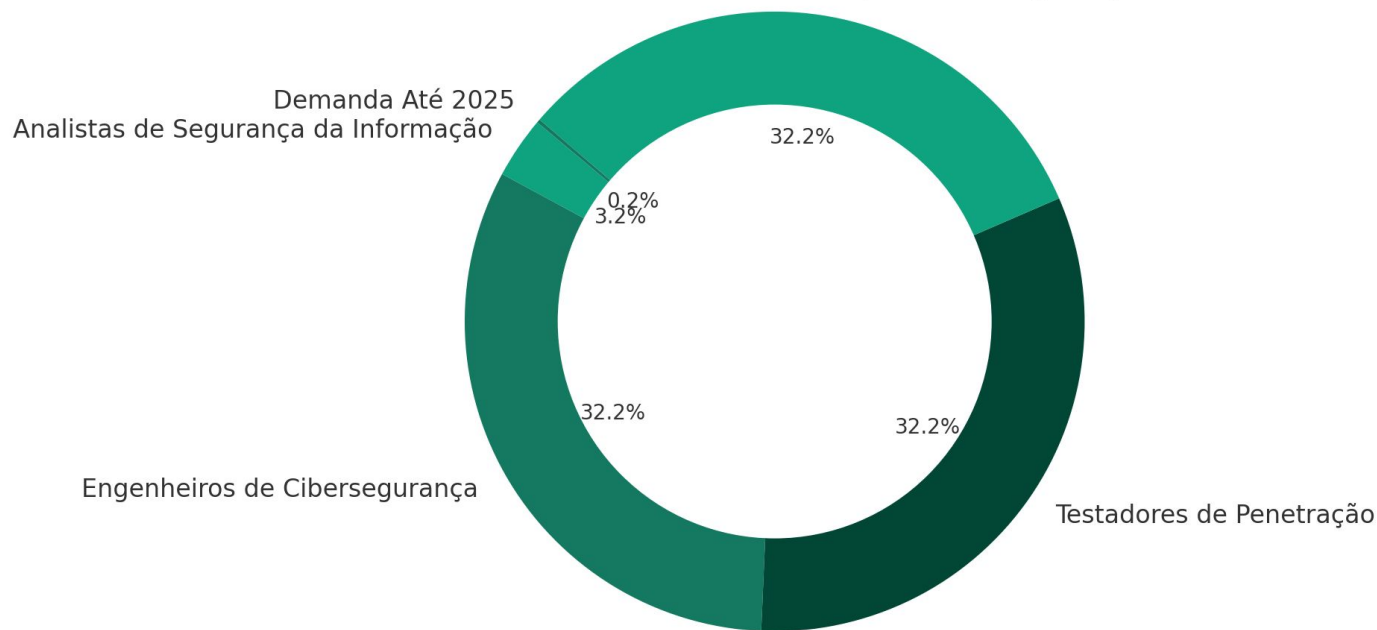
2023

Tendências do Mercado de Trabalho em Cibersegurança para 2023



2024-2028

Projeções de Empregabilidade em Cibersegurança (2024-2028)

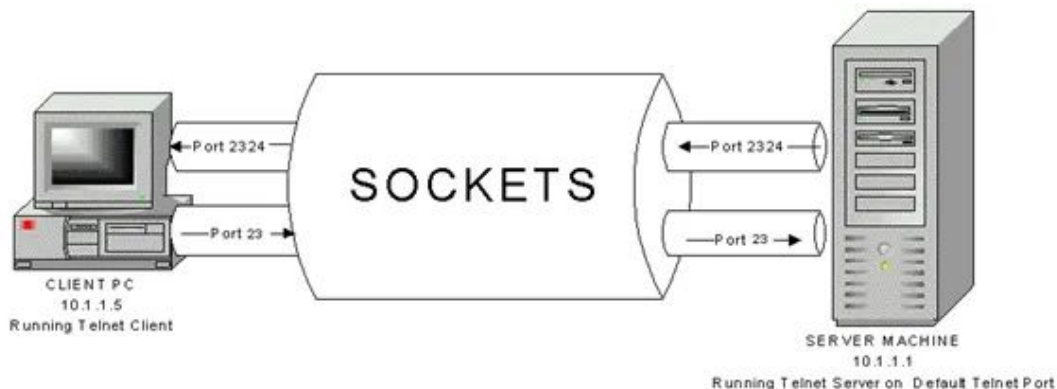


Socket - Python

Sockets são ferramentas que possibilitam a **interação** entre **dois** processos (**aplicativos**) distintos, seja no mesmo dispositivo ou em equipamentos separados. Isso implica que os Sockets são empregados para **facilitar** a comunicação entre diversos **computadores** ou entre dois **aplicativos** (processos) que operam simultaneamente no mesmo dispositivo.

Socket - Python

A imagem ilustra a **comunicação** via **socket** entre **dois computadores** diferentes. Neste processo, o computador cliente inicia a comunicação, enquanto o servidor aguarda por solicitações do cliente. Cada comunicação utiliza uma "**Porta**", um número que permite múltiplas comunicações em cada computador sem interferências entre elas. No exemplo, o Cliente usa o Socket na Porta **23** para se comunicar com o Servidor, que responde através de um Socket na Porta 2324.

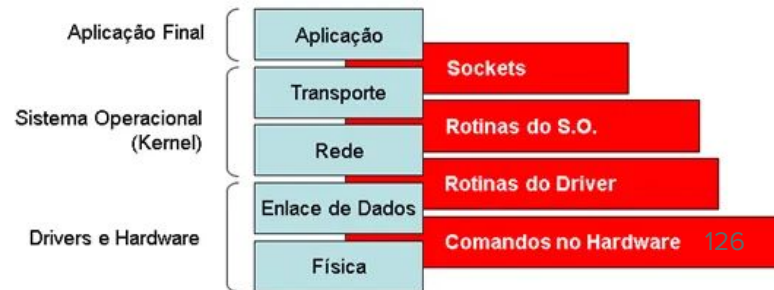


Socket - Python

Quando você digita um endereço web (www.google.com.br) em seu navegador, ele cria um Socket. Neste cenário, você atua como Cliente e o computador onde a página está armazenada é o Servidor. Durante este processo, várias etapas ocorrem internamente nos sistemas operacionais (Windows, Linux, Mac) tanto do Servidor quanto do Cliente, embora o usuário final (você) não perceba.

Socket - Python

A figura demonstra as etapas da comunicação via Socket em cada computador. No lado do Cliente, o navegador funciona como uma interface gráfica que interage com a camada de **Aplicação** do sistema operacional, solicitando a criação de um Socket. Cada camada do sistema (**Aplicação**, **Sistema Operacional**, **Drivers/Hardware**) executa um serviço específico, configura-o e o transmite para a próxima camada. Essas camadas são classificadas de acordo com sua função: **Aplicação Final (Navegador)**, **Sistema Operacional (Windows, Linux, Mac)** e **Drivers/Hardware** (componentes físicos do computador, como a placa de rede).



Vamos colocar a mão na massa!

Mas antes, vamos observar o que é solicitado.

[SocketPython](#)

A Aventura de uma mensagem pela Internet

Imagine que estamos embarcando em uma jornada pelo vasto mundo da Internet. Nossa missão é enviar uma mensagem até o grande servidor do **Google** e trazer de volta uma **resposta**. Para isso, vamos usar uma ferramenta poderosa: o **socket**.

→ Importação e Definição do Alvo:

- ◆ Primeiro, precisamos das ferramentas certas. Aqui, importamos o módulo **socket**, que é como uma mochila cheia de ferramentas para se comunicar pela Internet.
- ◆ Nosso destino? O famoso **www.google.com**, na porta **80**, a porta padrão para a comunicação web não segura.

→ Criando nosso Veículo de Comunicação (Socket):

- ◆ Agora, construímos nosso veículo, o socket. Pense nele como um pequeno drone que pode voar pela Internet.
- ◆ Configuramos para usar **IPv4 (AF_INET)** e para ser um veículo confiável e de conexão contínua (**SOCK_STREAM**, ou seja, **TCP**).

Continuação

→ Partindo para o Google:

- ◆ Com nosso drone pronto, conectamos ao Google. Aqui, `client.connect` é como dizer ao drone para voar até o servidor do Google.

→ Enviando a Mensagem:

- ◆ Precisamos de uma mensagem para enviar. Usamos um formato especial, chamado `HTTP`, que o Google entende. Aqui, estamos pedindo a página principal do Google (`GET / HTTP/1.1`).
- ◆ Enviamos a mensagem. Nosso drone agora está levando nossa solicitação pelo vasto oceano da Internet.

→ Aguardando a Resposta:

- ◆ Após o envio, esperamos. O drone coleta a resposta do Google e a traz de volta para nós.

→ Revelando a Mensagem do Google:

- ◆ Finalmente, imprimimos a resposta. O que será que o Google nos enviou de volta?

Resposta do Google!

→ Cabeçalhos HTTP:

- ◆ **Date, Expires, Cache-Control:** Informam sobre a data da resposta, a data de expiração e as diretrizes de cache.
- ◆ **Content-Type:** text/html; charset=ISO-8859-1: Especifica que o tipo de conteúdo da resposta é HTML e o conjunto de caracteres é ISO-8859-1.
- ◆ **Content-Security-Policy-Report-Only:** Define a política de segurança de conteúdo do site.
- ◆ **Server:** gws: Indica que o servidor é um servidor Google Web Server (gws).
- ◆ **Set-Cookie:** Esses cabeçalhos definem cookies que podem ser usados para manter o estado da sessão ou outras informações.
- ◆ **X-XSS-Protection, X-Frame-Options:** Cabeçalhos relacionados à segurança.

Resposta do Google!

→ Status da Resposta: HTTP/1.1 200 OK

- ◆ **HTTP/1.1** indica que a resposta está usando a versão 1.1 do protocolo HTTP.
- ◆ **200 OK** é um código de status HTTP que indica que a solicitação foi bem-sucedida e o servidor transmitiu a resposta solicitada.

→ Corpo da Resposta:

- ◆ O corpo da resposta contém o HTML da página inicial do Google. Inclui várias tags HTML (**<html>**, **<head>**, **<body>**, etc.), metadados (como **<meta>** e **<title>**), e scripts JavaScript.
- ◆ A parte inicial do HTML inclui informações sobre o layout da página, estilo CSS, e meta tags para SEO e configurações de mídia social.