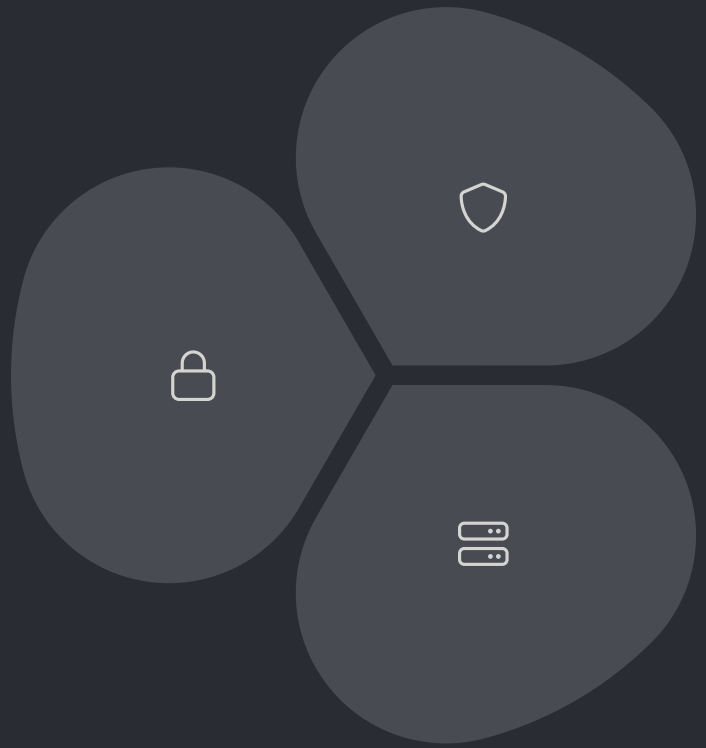
Treinamento de Conscientização sobre Segurança

R by Ricardo Tassio

O que é Segurança da Informação?

Confidencialidade

Acesso restrito a informações



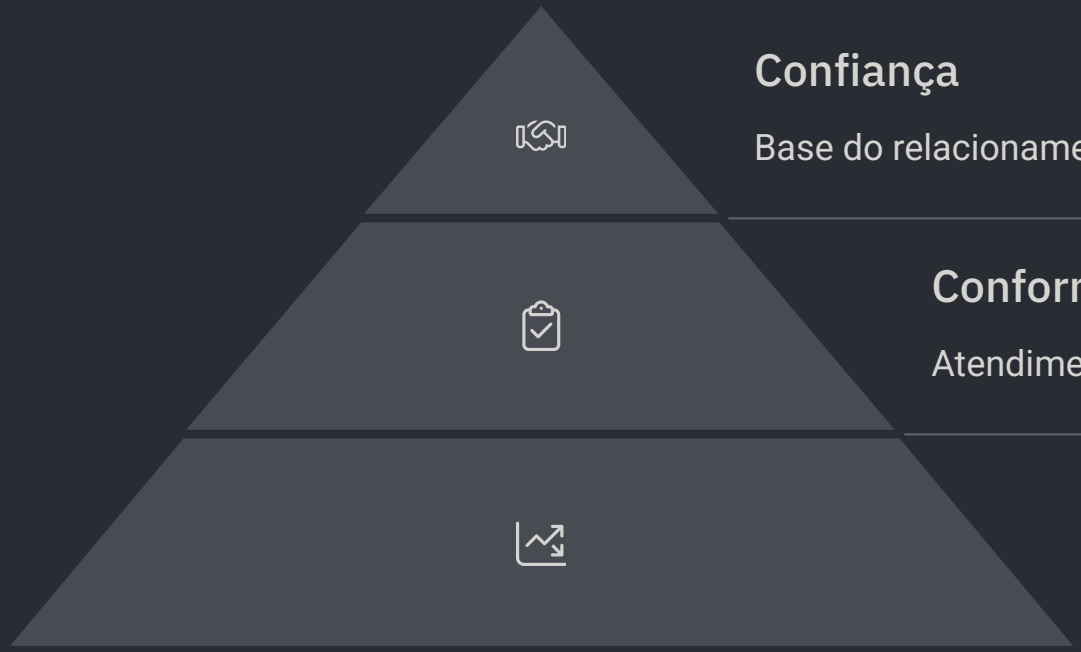
Integridade

Dados precisos e confiáveis

Disponibilidade

Acesso quando necessário

Por que a Segurança da Informação é Crucial



Confiança

Base do relacionamento com clientes

Conformidade

Atendimento às regulamentações

Continuidade

Manutenção das operações

Objetivos da Segurança Cibernética

Confidencialidade

Proteção de dados sensíveis

Ex: Criptografia de dados

Disponibilidade

Sistemas sempre acessíveis

Ex: Backup e redundância

Integridade

Dados precisos e inalterados

Ex: Verificação de assinaturas

Práticas Essenciais de Segurança

Engenharia Social

Reconhecer manipulação psicológica

Segurança de Senha

Senhas fortes e únicas

Autenticação Multifator

Adicionar camada extra de segurança

Segurança Física

Proteger acesso físico aos dispositivos

Protegendo-se contra Ameaças de E-mail

O que fazer

- Verificar remetentes
- Reportar e-mails suspeitos
- Verificar erros e logotipos

O que não fazer

- Não abrir anexos suspeitos
- Não compartilhar credenciais
- Evitar clicar em links duvidosos

Tipos de Ameaças de E-mail

Phishing

Imitação de entidades legítimas

Golpes

Fraudes financeiras

Spear Phishing

Ataques direcionados

Vírus e Malware

Códigos maliciosos

Spoofing

Falsificação de identidade

Navegação Segura na Web

Verificar URLs

Passar o mouse sobre links antes de clicar

Confirmar HTTPS

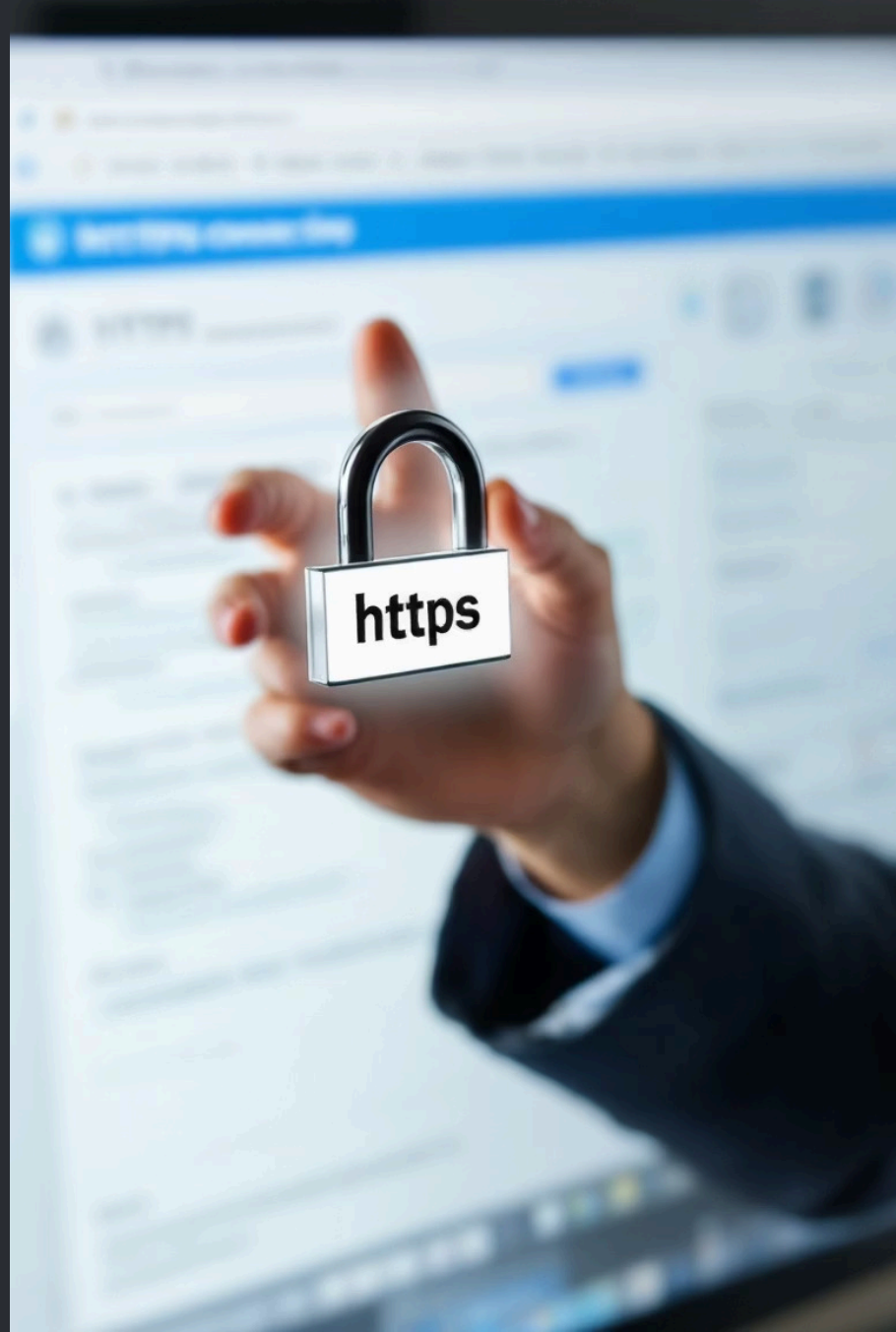
Buscar o cadeado na barra de endereços

Manter Atualizado

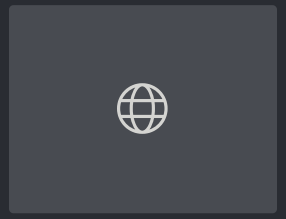
Atualizar navegadores e plugins regularmente

Usar Bloqueadores

Instalar bloqueadores de anúncios e scripts



Classificação de Dados

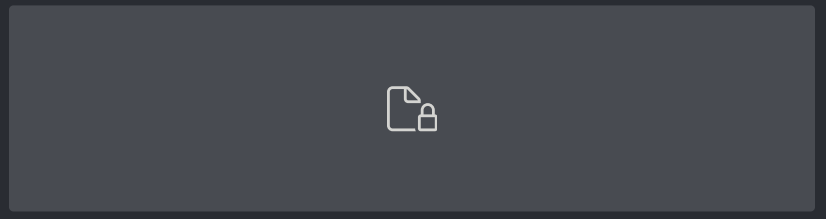


Dados Públicos

Informações disponíveis para todos

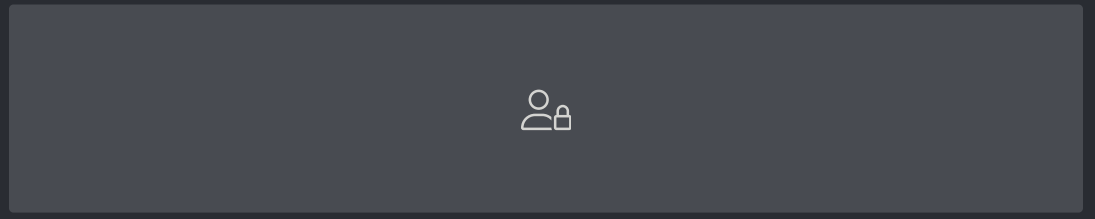
Dados Internos

Uso restrito à empresa



Dados Confidenciais da Empresa

Acesso limitado dentro da organização



Dados Confidenciais do Cliente

Máxima proteção necessária

Conscientização sobre Segurança é Responsabilidade de Todos

A segurança da informação depende de cada um de nós. Juntos, formamos a primeira linha de defesa contra ameaças cibernéticas.

Mantenha-se Vigilante

Questione situações suspeitas. Sua intuição geralmente está correta.

Comunique Incidentes

Reporte imediatamente qualquer atividade suspeita à equipe de TI.

Aprimore seu Conhecimento

Participe de treinamentos e atualizações sobre segurança regularmente.

Lembre-se: a segurança não é apenas tecnologia, mas principalmente comportamento.

Elementos de Risco

Ameaças

- Hackers e cibercriminosos
- Malware avançado
- Ataques internos
- Engenharia social

Vulnerabilidades

- Sistemas desatualizados
- Senhas fracas
- Falhas de configuração
- Treinamento insuficiente

Probabilidade

Análise baseada em histórico de incidentes e inteligência de ameaças atuais.

Impacto ao Negócio

Perdas financeiras, danos à reputação e possíveis sanções regulatórias.

Etapas para Proteger Sua Organização

Identificar Ativos

Mapeie todos os recursos críticos da empresa. Inclua sistemas, dados e dispositivos.

Avaliar Valor

Determine a importância de cada ativo para as operações. Quantifique seu valor para o negócio.

Documentar Impactos

Analise consequências de possíveis violações. Registre efeitos operacionais e financeiros potenciais.

Identificar Riscos

Reconheça ameaças específicas para cada ativo. Documente vulnerabilidades existentes e potenciais.

Priorizar Mitigação

Crie planos para os riscos mais críticos primeiro. Implemente controles considerando custo-benefício.

Detalhes das Etapas de Proteção

Inventário Detalhado

Crie um registro completo de todos ativos digitais e físicos. Atualize regularmente para incluir novos recursos tecnológicos.

Análise de Vulnerabilidades

Realize varreduras de segurança frequentes. Identifique pontos fracos antes que invasores os explorem.

Implementação de Controles

Aplique medidas técnicas como criptografia e autenticação multifator. Estabeleça políticas claras para todos os funcionários.

Monitoramento Contínuo

Instale sistemas de detecção de intrusão. Analise logs de segurança regularmente para identificar atividades suspeitas.

Resposta a Incidentes

Desenvolva protocolos para reação imediata às violações. Conduza exercícios simulados para testar sua preparação.

Top 10 Riscos - OWASP

O OWASP (Open Web Application Security Project) é uma comunidade global que trabalha para melhorar a segurança de software. Seu relatório Top 10 identifica os riscos mais críticos para aplicações web.

1. **Quebra de Controle de Acesso:** Permissões inadequadas que permitem acesso não autorizado
2. **Falhas Criptográficas:** Proteção insuficiente de dados sensíveis
3. **Injeção:** Inserção de código malicioso via entradas não sanitizadas
4. **Design Inseguro:** Falhas na arquitetura de segurança do sistema
5. **Configuração Incorreta:** Ajustes inadequados em servidores e aplicações
6. **Componentes Vulneráveis:** Uso de bibliotecas e frameworks desatualizados
7. **Falhas de Identificação:** Problemas com autenticação e sessões
8. **Falhas de Integridade:** Verificação insuficiente de dados e software
9. **Falhas de Logging:** Monitoramento inadequado de atividades suspeitas
10. **Falsificação de Requisições:** Execução de ações não autorizadas via CSRF

Por que Abordar o OWASP Top 10?

Ameaças Comuns

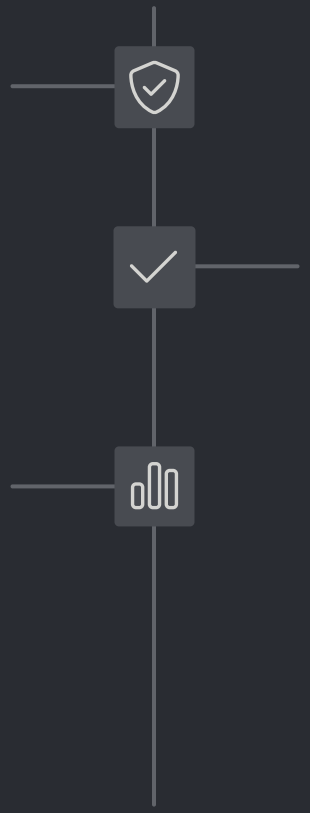
Os riscos do OWASP são as vulnerabilidades mais exploradas, sendo alvos frequentes de ataques.

Proteger-se contra eles é crucial para a segurança web.

Impacto Financeiro e de Reputação

A exploração dessas falhas pode resultar em perdas financeiras significativas.

Incidentes afetam a confiança do cliente e a reputação da empresa.



Conformidade Regulatória

Diversas regulamentações exigem proteção contra as vulnerabilidades identificadas pelo OWASP.

Estar em conformidade garante a segurança e evita penalidades.

Conclusão

Segurança é Contínua

A proteção de dados requer vigilância constante. Mantenha-se atualizado sobre novas ameaças.

Conscientização é Fundamental

Todos são responsáveis pela segurança da informação. Um único erro pode comprometer toda a organização.

Implemente o OWASP Top 10

Corrija as vulnerabilidades mais críticas primeiro. Realize auditorias de segurança regularmente.

Cultura de Segurança

Promova uma postura proativa em relação à segurança. Recompense boas práticas de segurança.

Lembre-se: a segurança não é apenas uma questão técnica, mas organizacional. Invista em treinamentos regulares e mantenha canais abertos para relatar incidentes suspeitos.