IDENTIFICAR VULNERABILIDADES E REFORÇAR A SEGURANÇA DA SUA ORGANIZAÇÃO

Auditoria de Cibersegurança

SABER MAIS



TAC Auditoria de Cibersegurança

TRIGÉNIUS TECNOLOGIA

AUDITORIA DE CIBERSEGURANÇA

OS CIBERATAQUES EM PORTUGAL AUMENTARAM MAIS DE 716% DE 2015 A 2023

Os criminosos estão cada vez mais sofisticados a explorar falhas como passwords fracas, softwares desatualizados, ou definições de segurança mal configuradas.

PRINCIPAIS TIPO DE INCIDENTES EM PORTUGAL

Phishing/Smishing	35%
Tentativa de login	19%
Engenharia Social	10%
Comprometimento de conta não privilegiada	7%
Distribuição de malware	6%
Utilização ilegítima de nome de terceiro	5%
Sistema infetado (malware)	4%
Sistema vulnerável	3%
Modificação não autorizada (ransomware)	3%
Comprometimento de aplicação	2%

Registados pelo CERT.PT em 2023

CENÁRIO GLOBAL

59% **De todas as organizações** foram atingidas por ataques de ransomware no último ano.

1/3 **De todos os ciberataques** são de phishing, o que o faz o método de ataque por correio eletrónico mais comum.

70% **Das violações de dados** causaram interrupções significativas ou muito significativas.

41% **Das pequenas empresas** sofreram uma ameaça cibernética.

350% **Mais ataques de engenharia social atingem pequenas empresas** do que grandes empresas, muitos deles vindos de imitadores da Microsoft.

AS **PMEs** SÃO MAIS SUSCEPTÍVEIS DE SEREM ALVO DE TENTATIVAS DE PHISHING

TRIGÉNIUS TECNOLOGIA

Falamos?
Solicite contacto ou agende uma demonstração.

AUDITORIA DE CIBERSEGURANÇA

IMPLEMENTE PROCESSOS DE AUDITORIA ROBUSTOS NA SUA ORGANIZAÇÃO

Garanta uma avaliação estruturada e eficaz com as seguintes etapas.

ETAPAS DO PROCESSO

INQUÉRITO

Antes da realização da primeira reunião, um questionário pré-auditoria será enviado ao cliente.

DEFINIÇÃO DE OBJETIVOS

Serão identificadas as principais prioridades, riscos e objetivos do cliente em matéria de cibersegurança.

AUDITORIA

Verificação dos controlos definidos no QNRCS, recolha de informações e realização de testes de segurança.

RELATÓRIO

Será elaborado um relatório conciso com os principais resultados, conclusões e recomendações.

ADD-ON OPCIONAL

Intervenção sobre incidências, com ações corretivas recorrendo aos serviços de cibersegurança Trigénius.

PRINCIPAIS CARACTERÍSTICAS

Planeamento e Preparação
Este plano não só garante que as auditorias são realizadas de forma eficiente, como também se alinha com os objetivos organizacionais e os requisitos de Conformidade

Recolha de Informações e Identificação de Ativos
O objetivo é mapear a infraestrutura de rede, identificar dispositivos e serviços ativos, descobrir potenciais vulnerabilidades e recolher informações sobre os indivíduos e a organização

Resultados e Recomendações
Após a conclusão da auditoria, será produzido um relatório detalhado que consolida todas as análises descobertas e recomendações

Avaliação dos Controlos de Segurança
Durante a auditoria, será avaliado se os controlos de segurança da organização, conforme definidos no Quadro Nacional de Referência para a Cibersegurança (QNRCS), estão implementados e abrangem os aspetos técnicos necessários para assegurar uma postura de segurança robusta

Identificação e Avaliação de Riscos
A identificação e avaliação de riscos constitui um processo sistemático destinado a identificar e analisar os riscos que podem afetar os ativos, as operações e a reputação de uma organização, servindo de base para a sua gestão eficaz

TRIGÉNIUS TECNOLOGIA

Trigénius Tecnologia...

AUDITORIA DE CIBERSEGURANÇA

AUDITORIA EM CONFORMIDADE COM AS NORMAS CERTIFICADAS

Este plano estabelece diretrizes claras e define o âmbito e a logística da auditoria, assegurando que todas as ações são executadas dentro de uma estrutura definida e controlada.

SEGUIMOS O STANDARDS DA INDÚSTRIA

A nossa abordagem à auditoria de cibersegurança baseia-se nos mais reconhecidos standards internacionais e nacionais, garantindo **rigor, abrangência e alinhamento com as melhores práticas do setor.**

A auditoria é conduzida de acordo com as orientações estabelecidos por:

- National Institute of Standards and Technology (NIST) 800-115;
- ISO 27001;
- Quadro Nacional de Referência para a Cibersegurança (QNRCS).

RECOLHA DE INFORMAÇÕES E IDENTIFICAÇÃO DE ATIVOS

FOOTPRINTING DIGITAL

Dados e informações digitais rastreáveis que os indivíduos, organizações ou sistemas deixam para trás como resultado das suas atividades online.

Abrange tanto os dados partilhados ativamente pelo utilizador como os dados passivos gerados através do comportamento online.

DESCOBERTA DA REDE

Processo fundamental para compreender a dinâmica da rede, através de técnicas passivas.

Ajudar na identificação de dispositivos não autorizados, sistemas operativos desconhecidos e atividades invulgares.

Integrados na gestão de rede, detetam novos dispositivos e mantêm o mapa de rede atualizado, reforçando a segurança.

ANÁLISE DE VULNERABILIDADES

Utilizada para identificar pontos fracos nos sistemas de uma organização.

A sua função principal é detetar potenciais problemas como software desatualizado, correções em falta e configurações incorretas.

TRIGÉNIUS TECNOLOGIA

Falamos?
Solicite contacto ou agende uma demonstração.

AUDITORIA DE CIBERSEGURANÇA

IDENTIFICAÇÃO, AVALIAÇÃO DE RISCOS E REALIZAÇÃO DE TESTES

Avaliação do potencial de perda ou dano quando uma ameaça explora uma vulnerabilidade num sistema de informação.

OS PRINCIPAIS FATORES DO RISCO

- A probabilidade de ocorrência de um evento;
- O potencial impacto nos ativos, operações ou indivíduos de uma organização.

TESTES DE SEGURANÇA

TESTES DE SEGURANÇA DE CREDENCIAIS

Durante a auditoria, serão realizados testes para avaliar a segurança das credenciais de autenticação da organização.

TESTES DE PENETRAÇÃO (IN.LOCO)

Avaliam a eficácia da segurança física ao simular acessos não autorizados, como ligações diretas à rede, roubo de dados ou instalação de dispositivos maliciosos.

TESTES DE PENETRAÇÃO

Simulam ataques reais para identificar vulnerabilidades em redes, sistemas e aplicações.

Permitem avaliar a eficácia das defesas, seja a partir do exterior (sem acesso prévio) ou do interior da organização.

TESTES DE ENGENHARIA SOCIAL

Avaliação do aspeto humano da segurança e a consciencialização dos utilizadores, destacando os pontos fracos do comportamento, como a incapacidade de aderir aos procedimentos estabelecidos.

Após a Execução dos Testes

OS RESULTADOS SÃO CONSOLIDADOS NUM **RELATÓRIO DETALHADO**

Este relatório descreve as vulnerabilidades identificadas, e as avaliações de risco.

Esta documentação permite às organizações compreenderem os riscos associados às vulnerabilidades encontradas.

TRIGÉNIUS TECNOLOGIA

Trigénius Tecnologia...

AUDITORIA DE CIBERSEGURANÇA

A PREVENÇÃO COMEÇA COM UMA AVALIAÇÃO COMPLETA DA SUA SEGURANÇA

Desde a fase de planeamento até à análise final de resultados, garantindo uma avaliação rigorosa da postura de segurança da informação.

PLANEAMENTO E PREPARAÇÃO

- Questionário Pré-Auditoria
- Desenvolvimento do Plano de Auditoria de Segurança
- Priorização e Agendamento dos Sistemas
- Considerações Legais

AVALIAÇÃO DOS CONTROLOS DE SEGURANÇA

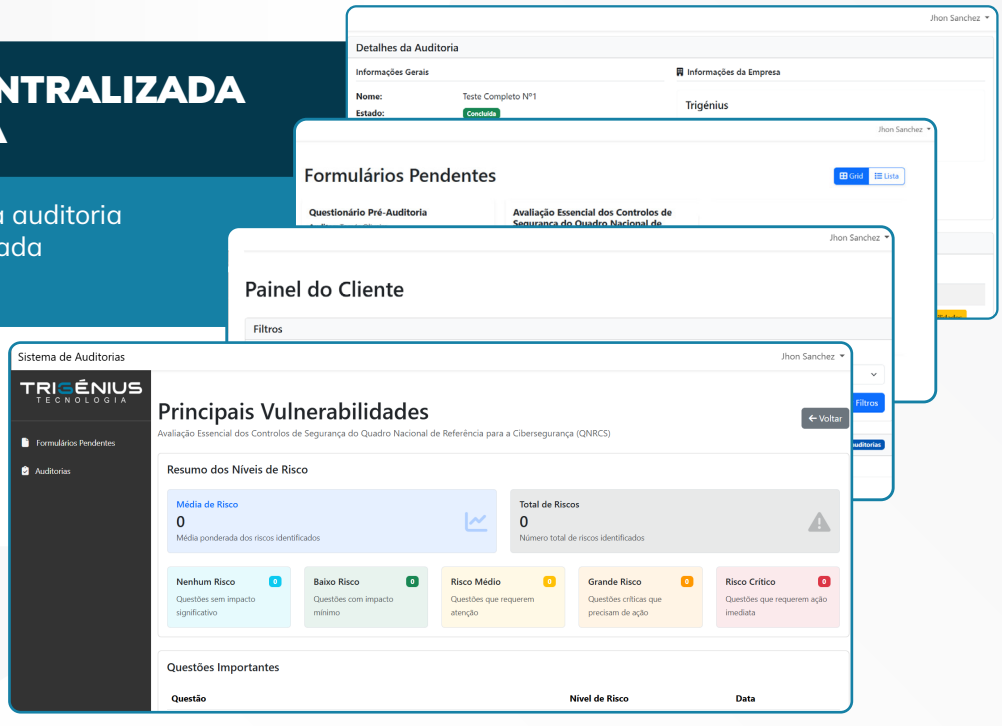
- Revisão de Controlos e Procedimentos
- Avaliação dos Controlos

RECOLHA DE INFORMAÇÕES E IDENTIFICAÇÃO DE ATIVOS

- Footprinting Digital
- Descoberta da Rede
- Enumeração da Rede e Serviços
- Análise de Vulnerabilidades

PLATAFORMA CENTRALIZADA PARA AUDITORIA

Onde toda a informação da auditoria é organizada e disponibilizada de forma segura.



Página dedicas a gestão de:

- Auditorias
- Avaliações
- Formulários
- Vulnerabilidades

TRIGÉNIUS TECNOLOGIA

AUDITORIA DE CIBERSEGURANÇA

A SUA CIBERSEGURANÇA ESTÁ EM PRIMEIRO LUGAR FAÇA UMA AUDITORIA AGORA

O objetivo da auditoria é identificar vulnerabilidades, avaliar a implementação dos controlos de segurança e fornecer recomendações claras para reforçar a segurança da organização.

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

- Testes de Segurança de Credenciais
- Testes de Penetração no Local
- Testes de Engenharia Social
- Verificação de Vulnerabilidades de Sistemas e Aplicações
- Teste de Penetração
- Classificação e Priorização de Riscos
- Mitigação e Recomendações

RESULTADOS E RECOMENDAÇÕES

- Relatório de Auditoria
- Melhoria Contínua

GESTÃO DE DADOS

Os dados organizacionais serão armazenados, transmitidos e removidos após a auditoria, **garantindo a conformidade com as políticas organizacionais relevantes**, como o RGPD ou normas semelhantes.

Falamos?
Solicite contacto ou agende uma demonstração.

TRIGÉNIUS TECNOLOGIA

ENTÃO, ESTÁ DECIDIDO? FALE CONNOSCO. AVANCE.

Somos todos ouvidos.

CLIQUE AQUI

trigenius.pt

Escolha online o que prefere:
Agendar Reunião | Solicitar Visita
Chamada Telefónica | Contacto por e-mail

TRIGÉNIUS
TECNOLOGIA

contacto@trigenius.pt
+351 249 530 800
Fátima, Lisboa

v.01-07.2025