



CYBERSECURITY AWARENESS

PROFESSIONAL CERTIFICATION



CAPC™ Versão 072024



...

Certificação Profissional de Conscientização em Segurança Cibernética (CAPC)

CAPC™ Versão 072024



Quem é Certiprof®?

Certiprof® é um órgão organismo de certificação fundado nos Estados Unidos em 2015, atualmente localizada em Sunrise, Flórida.

Nossa filosofia se baseia-se na criação de conhecimento em comunidade e, para isso, sua rede colaborativa é composta por:

- **Nossos Lifelong Learners (LLL)** se identificam como Continuous Learners (Alunos Contínuos), demonstram seu compromisso inabalável com o aprendizado contínuo, que é de vital importância no mundo digital atual, em constante mudança e expansão. Independentemente de serem aprovados ou não o exame.
- Universidades, centros de treinamento e facilitadores de todo o mundo fazem parte de nossa rede de **CPLS (Certified Partner For Learning Solutions)**.
- **Os autores (co-criadores)** são especialistas ou profissionais do setor que, com seu conhecimento, desenvolvem conteúdo para a criação de novas certificações que atendem às necessidades do setor.
- **Equipe interna:** nossa equipe distribuída com operações na Índia, no Brasil, na Colômbia e nos Estados Unidos é encarregada de superar obstáculos, encontrar soluções e fornecer resultados excepcionais.



Nossas Afiliações

Memberships



Digital badges issued by



IT Certification Council – ITCC

Certiprof® é um membro ativo do ITCC.

Um dos aspectos importantes de fazer parte do ITCC é a forma como os líderes do setor colaboram entre si em um formato aberto para explorar maneiras novas ou diferentes de fazer negócios que inspiram e incentivam a inovação, estabelecendo e compartilhando práticas recomendadas que nos permitem estender esse conhecimento à nossa comunidade. A Certiprof contribuiu com livros brancos na Career Path Ways Taskforce, uma força-tarefa que foi implementada internamente para oferecer aos alunos a oportunidade de saber que caminho seguir após uma certificação.

- **IBM**
- **CISCO**
- **ADOBE**
- **AWS**
- **SAP**
- **GOOGLE**
- **ISACA**



Certiprof® é um membro corporativo da Agile Alliance.

Ao aderir ao programa corporativo da Agile Alliance, continuamos a capacitar as pessoas, ajudando-as a atingir seu potencial por meio da educação. Todos os dias, fornecemos mais ferramentas e recursos que permitem que nossos parceiros treinem profissionais que buscam aprimorar seu desenvolvimento e suas habilidades profissionais.

<https://www.agilealliance.org/organizations/certiprof/>



Essa aliança permite que indivíduos e empresas certificados pela Certiprof® tenham uma distinção mundial por meio de um crachá digital.

A Credly é a maior emissora de crachás do mundo e as principais empresas de tecnologia, como IBM, Microsoft, PMI, Nokia, Universidade de Stanford, entre outras, emitem seus crachás com a Credly.

Empresas que emitem crachás de validação de conhecimento com a Credly:

- **IBM**
- **Microsoft**
- **PMI**
- **Universidad de Stanford**
- **Certiprof**



Selos digitais



Selos digitais:
o que são?

De acordo com o estudo do IT Certification Council (ITCC), anos atrás, as pessoas sabiam muito pouco sobre os selos digitais. Hoje, grandes empresas e instituições educacionais do mundo todo emitem selos.

Os selos digitais contêm metadados detalhados sobre quem os recebeu, as competências exigidas e a organização que os emitiu. Alguns selos estão até mesmo vinculados às atividades necessárias para obtê-los.

Para empresas e instituições educacionais, os selos e as informações que eles fornecem são tão importantes que muitas decisões, como as de recrutamento ou admissão, são baseadas nos dados que eles fornecem.



Por que eles são importantes?



- **Facilidade de compartilhamento e verificação de conquistas:**

Os selos digitais permitem que os profissionais mostrem e verifiquem suas conquistas instantânea e globalmente. De acordo com um relatório da Credly, **os perfis do LinkedIn com emblemas digitais recebem 40% mais atenção dos recrutadores e empregadores.**
- **Visibilidade em plataformas digitais:**

Em uma pesquisa realizada pela Pearson e pela Credly, **85%** dos usuários que ganharam selos digitais os **compartilharam no LinkedIn** e **75%** relataram que isso aumentou **a credibilidade profissional em suas redes.** Além disso, **76%** dos empregadores pesquisados disseram que os selos digitais os ajudam a identificar rapidamente habilidades específicas.



Por que eles são importantes?

- **Impacto na contratação:**

um estudo da **Associação Internacional de Gerenciamento de Projetos (PMI)** constatou que os candidatos que exibem selos digitais de gerenciamento de projetos têm 60% mais chances de serem contratados em comparação com aqueles que apenas mencionam suas habilidades sem verificação digital.



Por que eles são importantes?

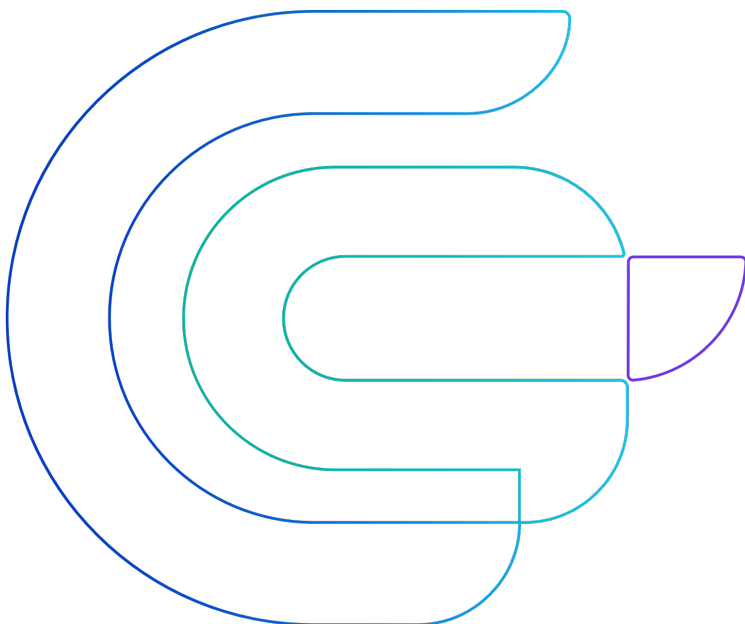


- **Fortalecimento da marca pessoal:**

A visibilidade e a verificação instantâneas proporcionadas pelos selos digitais permitem que os profissionais não apenas demonstrem suas habilidades, mas também criem uma marca pessoal forte. De acordo com um estudo do LinkedIn, os profissionais que usam selos digitais **têm 24%** mais chances de progredir em suas carreiras.

A certificação e os selos digitais não são apenas uma validação do conhecimento, mas também uma ferramenta poderosa para o aprimoramento contínuo e a empregabilidade. Em um mundo em que a aprendizagem contínua se tornou a norma, essas credenciais são fundamentais para o desenvolvimento profissional e a competitividade no mercado de trabalho global.





Nem todos os selos são iguais e, na **Certiprof**, temos o compromisso de oferecer a você mais do que apenas reconhecimento digital. Ao receber um selo emitido pelo **Certiprof**, você estará recebendo uma validação do seu conhecimento com o respaldo de um dos principais órgãos de certificação profissional do mundo.

Dê o próximo passo e obtenha o selo que abrirá portas e o posicionará como um especialista em sua área.



Por que é importante obter seu certificado?

- **Prova de experiência:** Seu certificado é um reconhecimento formal das habilidades e do conhecimento que você adquiriu. Ele serve como prova verificável de suas qualificações e demonstra seu compromisso com a excelência em sua área.
- **Credibilidade e reconhecimento:** no mercado de trabalho competitivo de hoje, os empregadores e colegas valorizam as credenciais que o diferenciam dos demais. Um certificado de uma instituição reconhecida, como o Certiprof, proporciona credibilidade instantânea e aumenta sua reputação profissional.
- **Avanço na carreira:** ter seu certificado pode abrir portas para novas oportunidades. Seja uma promoção, um aumento de salário ou um novo emprego, as certificações são um diferencial importante que os empregadores consideram ao avaliar os candidatos.



Por que é importante pagar por seu certificado:

- **Oportunidades de networking:** Ter uma certificação o conecta a uma rede de profissionais certificados. Muitas organizações têm grupos de ex-alunos ou de networking onde você pode compartilhar experiências, trocar ideias e expandir seu círculo profissional.
- **Realização pessoal:** obter uma certificação é uma grande conquista, e seu certificado é um lembrete tangível do trabalho árduo, da dedicação e do progresso que você fez. É algo de que você pode se orgulhar e mostrar aos outros.





Earn this Badge

Cybersecurity Awareness Professional Certification - CAPC

Issued by [Certiprof](#)

The holders of this badge have validated and demonstrated a comprehensive understanding of cybersecurity principles and best practices. This badge highlights the individual's ability to recognize and address common cyber threats, implement effective protective measures, and contribute to a secure digital environment. They understand the importance of cybersecurity and its economic and legal implications.

[Learn more](#)

Certification

Advanced

Hours

Paid

Skills

Adapability

Collaboration

Communication

Critical Thinking

Incident Response

Leadership

Risk Management

<https://www.credly.com/org/certiprof/badge/cybersecurity-awareness-professional-certification->



Lifelong Learning

- O Certiprof criou um selo especial para reconhecer os alunos consistentes.
- Até 2024, mais de 1.000.000 desses crachás terão sido emitidos em mais de 11 idiomas.

Objetivo e filosofia

- Este selo é para pessoas que acreditam firmemente que a educação pode mudar vidas e transformar o mundo.
- A filosofia por trás do emblema é promover o compromisso com o aprendizado contínuo ao longo da vida.

Acesso e obtenção do crachá

- O selo Lifelong Learning é concedido gratuitamente àqueles que se identificam com essa abordagem de aprendizagem.
- Qualquer pessoa que se considere um aluno consistente pode reivindicar seu distintivo visitando o site:

<https://certiprof.com/pages/certiprof-lifelong-learning>



...

COMPARTILHE E VERIFIQUE
SUAS REALIZAÇÕES DE
APRENDIZAGEM
COM FACILIDADE

#CAPC #certiprof



 certiprof®

...

...

Módulo 1: Introdução à segurança cibernética



CAPC™ Versão 072024



Bem-vindo ao Curso de Conscientização sobre Segurança Cibernética e ao Programa de Certificação

- Introdução ao curso
- Estabelecendo as bases para o aprendizado em segurança cibernética
- Duração: 6 horas



Introdução do instrutor

- Nome: [Nome do instrutor]
- Histórico e experiência:
 - Experiência profissional
 - Principais realizações em segurança cibernética
 - Certificações e experiência relevante
- Informações de contato:
 - E-mail: [E-mail do instrutor] [E-mail do instrutor]
 - Horário e disponibilidade do escritório



Objetivos do curso



- Entendendo a importância da segurança cibernética
 - Por que a segurança cibernética é importante no mundo digital de hoje?
- Aprender sobre ameaças e vulnerabilidades comuns
 - Identificação de diferentes tipos de ameaças cibernéticas
 - Compreensão das vulnerabilidades comuns em sistemas e redes
- Implementar medidas de proteção
 - Práticas recomendadas para proteger dispositivos e informações
- Resposta eficaz a incidentes de segurança
 - Etapas a serem seguidas quando ocorrer uma violação de segurança
- Garantir a conformidade com as políticas e normas de segurança
 - Visão geral das principais leis e regulamentações de segurança cibernética



Expectativas do curso



Participação ativa:

- Participar de discussões e atividades
- Faça perguntas e compartilhe experiências



Participação ativa:

- Analise os materiais fornecidos
- Conclua as leituras e os exercícios designados



Avaliação:

- Passar no exame final de certificação
- Demonstrar compreensão dos principais conceitos por meio de testes e atividades.



Aprendizado contínuo:

- Manter-se atualizado com as últimas tendências e práticas em segurança cibernética



Por que essa certificação?

Top stories :
News about Microsoft • CrowdStrike >



CNN
¿Qué pasó con Microsoft en la caída global informática y qué causó el fallo?
21 hours ago

DW
La falla global en Microsoft tuvo antecedentes recientes
18 hours ago

Infobae
CrowdStrike aseguró que "el problema ha sido identificado, aislado y se ..."
10 hours ago

Semana.com
Crisis mundial en vuelos y aerolíneas por caída de Microsoft: hay caos en ...
18 hours ago

Política | ALEMANIA

Alemania convoca a embajador en Rusia por ciberataques rusos

DAVID GONZÁLEZ

Alemania y República Checa acusan al grupo APT28, dirigido por los servicios de inteligencia de Rusia, de una reciente campaña de ciberataques, acusaciones que Rusia considera "infundadas".

f x



Alexander Graf Lambsdorff, embajador de Alemania en México (imagen de archivo)

Publicación

El gobierno alemán indicó este lunes (04.05.2024) que había llamado a consultas a su embajador en **Rusia**, Alexander Graf Lambsdorff, después de haber acusado el viernes a un grupo de hackers rusos controlado por Moscú de una reciente campaña de ciberataques.

El embajador "permanecerá una semana en Berlín y después volverá a Moscú", indicó durante una rueda de prensa la portavoz del Ministerio de Relaciones Exteriores de **Alemania**, Kathrin Deschauer. El gobierno toma "muy en serio" este "acto contra nuestra democracia", agregó.

Los gobiernos alemán y checo acusaron el viernes al grupo APT28, dirigido por los servicios de inteligencia de Rusia, de una reciente campaña de ciberataques en sus países, acusaciones que Rusia considera "infundadas".

Según el gobierno alemán, se produjo en particular un ciberataque de direcciones de correo electrónico de responsables del Partido Socialdemócrata Alemán (SPD), del canciller **Olaf Scholz**.

Berlín anunció el viernes que **apoyó al encargo de negocios de la embajada de Rusia** "para hacer entender al gobierno ruso" que no acepta "estas acciones".

Desde el inicio de la invasión rusa de Ucrania en febrero de 2022, los países occidentales están en alerta máxima contra el riesgo de ataques informáticos masivos y de operaciones de desinformación dirigidas por Rusia.

m (afp/dpa)

El Banco Santander informa de un ciberataque que afecta a clientes y a toda la plantilla

El banco afirma que no se ha producido robo de contraseñas y que "los clientes pueden seguir operando con normalidad".



AGENCIAS / EFE / EL PAÍS

Publicado: 04/05/2024 13:12 (UTC+1)
Última actualización: 04/05/2024 14:35 (UTC+1)

Euskaraz irakurti: Santander bankuak bezeroei eta langile guztiei eragiten dien zibereraso baten berri eman du

El Banco Santander ha informado de un reciente "acceso no autorizado" a una base de datos de la entidad alojada en un proveedor que ha afectado a clientes de España, Chile y Uruguay, y a todos los empleados y a algunos empleados del grupo, según ha informado en un comunicado a la Comisión Nacional del Mercado de Valores (CNMV).

En el resto de mercados y negocios de la entidad no hay datos de clientes afectados. Santander señala que en la base de datos afectada no hay información transaccional ni credenciales de acceso o contraseñas de banca por internet que permitan operar con el banco.

"Las operaciones y los sistemas de Santander no están afectados y los clientes pueden seguir operando con seguridad", añade el banco.

El banco, que está llevando a cabo una investigación, señala que implementó "de inmediato" medidas para gestionar el incidente, como el bloqueo del acceso a la base de datos y un refuerzo de la prevención contra el fraude para proteger a los clientes.

Santander "lamenta" la situación y señala que está informando "proactivamente" a los clientes y empleados directamente afectados. "Hemos notificado oportunamente a reguladores y fuerzas de seguridad, y continuaremos colaborando con ellos", concluye el comunicado.



Por que você está no Certiprof?

A CertiProf tem participado ativamente da criação de materiais de segurança cibernética por meio de colaborações com organizações reconhecidas e do uso de estruturas estabelecidas.

Participação nos principais eventos de segurança cibernética

- O CertiProf é membro da National Cybersecurity Alliance e participa de iniciativas como o CyBOK (Cybersecurity Body of Knowledge), garantindo que seus materiais estejam alinhados com as práticas recomendadas e os mais recentes desenvolvimentos em segurança cibernética.

Uso de estruturas e padrões de referência internacionais

- Os materiais do CertiProf são baseados em estruturas reconhecidas, como as diretrizes do NIST (National Institute of Standards and Technology) e da Agência de Segurança do Governo dos EUA, garantindo que as certificações forneçam conhecimentos e habilidades atualizados e relevantes para os profissionais da área de segurança cibernética.



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CyBOK



**NATIONAL
CYBERSECURITY
ALLIANCE**



...

Módulo 2: Conceitos básicos de segurança cibernética



CAPC™ Versão 072024



Noções básicas de segurança cibernética



- Introdução aos conceitos fundamentais



- Entendendo os fundamentos da segurança cibernética



O que é segurança cibernética?



- **Definição:**

- A segurança cibernética é a prática de proteger sistemas, redes e softwares contra ataques digitais.

- **Áreas-chave:**

- Proteger informações confidenciais contra acesso não autorizado.
- Garantir a integridade e a disponibilidade dos dados.
- Proteja-se contra ameaças cibernéticas, como hacking, phishing e malware.



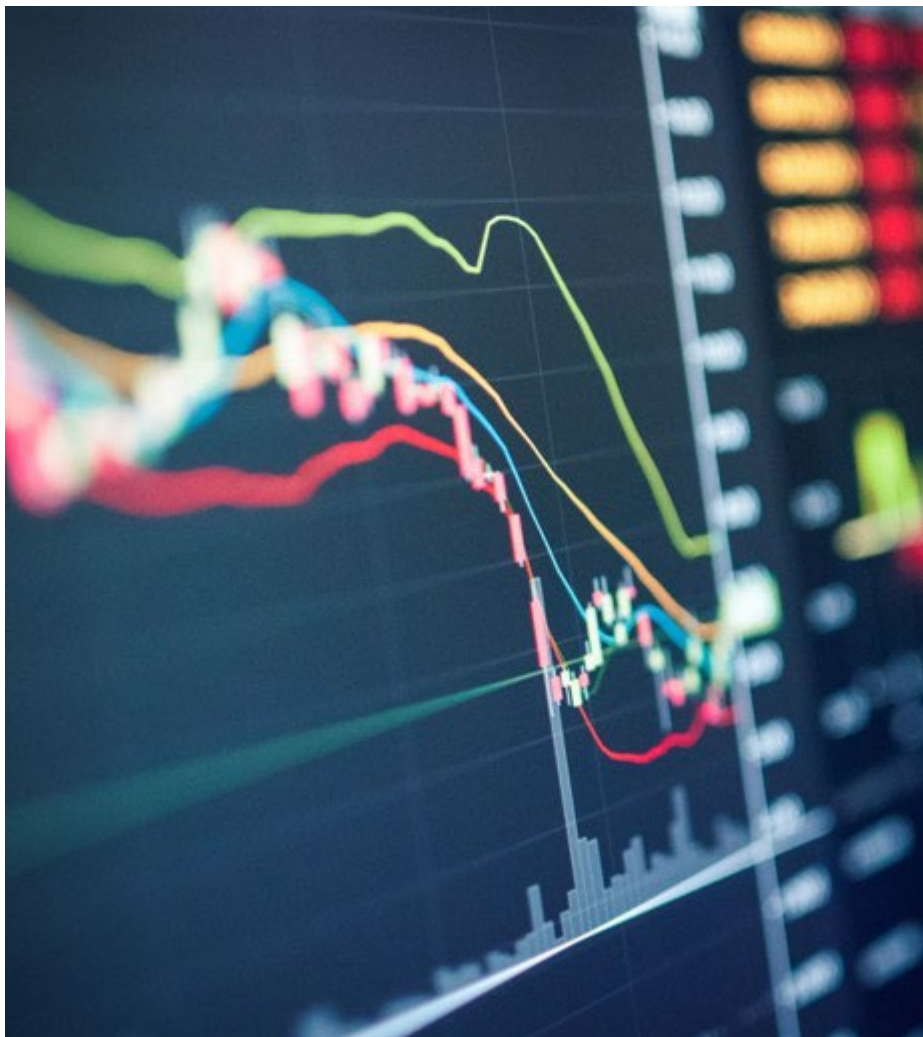
Importância da segurança cibernética no ambiente atual

- **Aumento das ameaças:**

- Crescimento das ameaças cibernéticas que afetam indivíduos, empresas e governos.
- Aumento de ataques sofisticados, como ransomware e ameaças persistentes avançadas (APTs).



Importância da segurança cibernética no ambiente atual



- **Impacto econômico:**

- Perdas financeiras devido a violações de dados e ataques cibernéticos.
- Custos de recuperação e danos à reputação das organizações.



Importância da segurança cibernética no ambiente atual

- **Requisitos legais e regulatórios:**

- Conformidade com leis como GDPR, HIPAA e outras normas de segurança cibernética.
- Importância de proteger os dados pessoais e manter a confiança do cliente.



Diferenças entre segurança cibernética e segurança da informação

- **Segurança cibernética:**

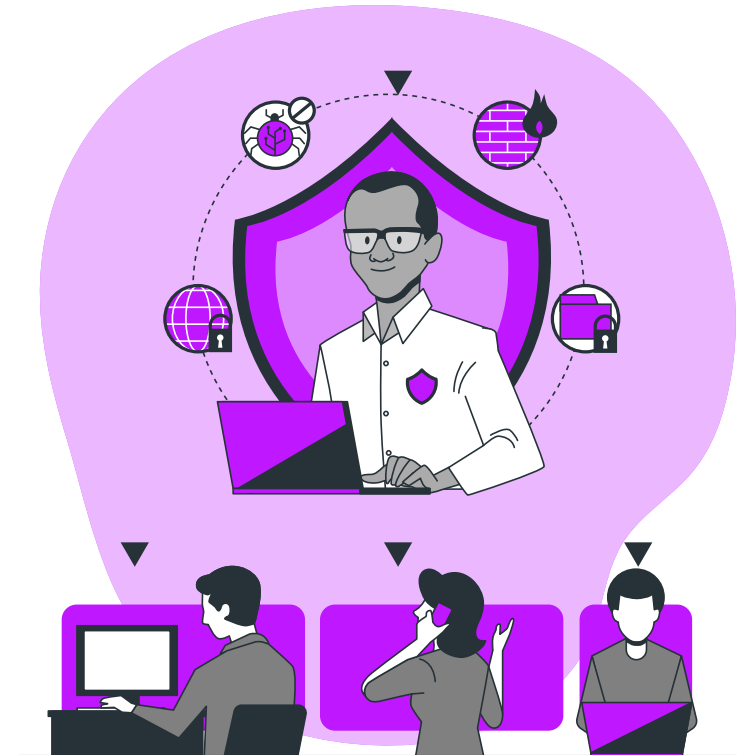
- Ele se concentra na proteção de dados e sistemas digitais contra ameaças cibernéticas.
- Ele inclui medidas de defesa contra hackers, malware e outros ataques cibernéticos.

- **Segurança da informação:**

- Escopo mais amplo, incluindo a proteção de todas as formas de informação (digital, física, etc.).
- Isso envolve garantir a confidencialidade, a integridade e a disponibilidade dos dados, independentemente do meio.

- **Sobreposição e integração:**

- A segurança cibernética é um subconjunto da segurança da informação.
- Ambos buscam proteger os ativos de informação, mas a partir de diferentes perspectivas e ameaças.



Ampliação dos conceitos-chave

Práticas de segurança cibernética:

- Implementação de firewalls, software antivírus e sistemas de detecção de intrusão (IDS).
- Realizar auditorias de segurança e avaliações de vulnerabilidade regulares.

Práticas de segurança da informação:

- Criptografia de dados, controles de acesso e medidas de segurança física.
- Desenvolvimento e implementação de políticas e procedimentos de segurança.

Por que ambos são importantes:

- Uma estratégia de segurança abrangente requer a integração de medidas de segurança cibernética e de segurança da informação.
- Uma abordagem holística garante a proteção contra uma ampla gama de ameaças, tanto digitais quanto físicas.



...

Módulo 3: Princípios de segurança cibernética



CAPC™ Versão 072024



Princípios de segurança cibernética



- **Compreensão dos conceitos básicos de segurança**



- **Estruturas e práticas essenciais**



Confidencialidade, integridade e disponibilidade (CIA)

- **Confidencialidade:**

- Definição: garantia de que as informações sejam acessíveis somente às pessoas autorizadas.
 - **Exemplos:** Criptografia, controles de acesso e mecanismos de autenticação.

- **Integridade:**

- Definição: garantir a precisão e a integridade dos dados.
 - **Exemplos:** Funções de hash, somas de verificação e controle de versão.

- **Disponibilidade:**

- Definição: garantia de que as informações e os recursos estejam disponíveis para os usuários autorizados quando necessário.
 - **Exemplos:** Redundância, mecanismos de failover e manutenção regular.



Princípios da Defesa em Profundidade

- **Segurança em camadas:**

- Definição: implementação de várias camadas de controles de segurança em um sistema de TI.
 - **Exemplos:** Firewalls, sistemas de detecção de intrusão (IDS) e software antivírus.

- **Múltiplas barreiras:**

- Conceito: nenhuma medida de segurança é infalível. Barreiras múltiplas aumentam a segurança.
 - **Exemplos:** Combinação de controles físicos, técnicos e administrativos.

- **Redundância e diversidade:**

- Redundância: ter sistemas e dados de backup para garantir a disponibilidade.
- Diversidade: uso de diferentes tipos de medidas de segurança para proteção contra uma variedade de ameaças.

- **Aplicação no mundo real:**

- **Exemplo:** uma empresa usa firewalls, sistemas de detecção de intrusão e treinamento regular de segurança para os funcionários.



Práticas recomendadas em segurança da informação

- **Políticas de senhas fortes:**

- Diretrizes: Use senhas complexas, altere-as regularmente e evite a reutilização.
 - **Ferramentas:** Gerenciadores de senhas para armazenar e gerar senhas com segurança.

- **Atualizações e patches regulares:**

- Importância: mantenha sistemas e softwares atualizados para se proteger contra vulnerabilidades.
 - **Prática:** implementação de um processo de gerenciamento de patches.

- **Educação e treinamento de usuários:**

- Foco: treinamento regular dos funcionários para que reconheçam tentativas de phishing e tratem as informações com segurança.
 - **Programas:** programas contínuos de conscientização sobre segurança cibernética.



Práticas recomendadas em segurança da informação

- **Controles de acesso:**

- Implementação: use o controle de acesso baseado em função (RBAC) para limitar o acesso com base nas funções do usuário.
 - **Exemplos:** Restringir o acesso a dados confidenciais somente àqueles que precisam deles.

- **Criptografia de dados:**

- Objetivo: proteger os dados em repouso e em trânsito.
- Ferramentas: use SSL/TLS para comunicações seguras e software de criptografia para armazenamento de dados.

- **Planejamento de resposta a incidentes:**

- Preparação: desenvolva e atualize regularmente um plano de resposta a incidentes.
- Etapas: Identificar, responder e se recuperar de incidentes de segurança.



Ampliação das principais práticas

- **Monitoramento contínuo:**

- Ferramentas: implemente sistemas de gerenciamento de eventos e informações de segurança (SIEM).
- Benefícios: Análise em tempo real de alertas de segurança e detecção proativa de ameaças.

- **Medidas de segurança física:**

- Controles: implemente controles de acesso, monitoramento e descarte seguro de documentos físicos.
- Importância: garantir que o acesso físico a sistemas e dados confidenciais seja restrito.



Ampliação das principais práticas

- **Auditoria e conformidade:**

- Processos: Realize auditorias de segurança e verificações de conformidade regulares.
- Padrões: aderir aos padrões do setor, como ISO 27001, NIST e GDPR.

- **Gerenciamento de riscos:**

- Abordagem: Identificar, avaliar e mitigar riscos.
- Ferramentas: use estruturas de avaliação de riscos e revise regularmente as estratégias de gerenciamento de riscos.



O que é o NIST (Instituto Nacional de Padrões e Tecnologia)?

O NIST é um órgão do Departamento de Comércio dos EUA que desenvolve e promove padrões de tecnologia, metrologia e inovação para melhorar a competitividade e a qualidade de vida dos americanos.

O NIST fornece diretrizes e padrões amplamente reconhecidos e usados no setor de segurança cibernética, como o Cybersecurity Framework, que ajuda as organizações a gerenciar e reduzir os riscos de segurança cibernética.

Importância da função de líder de segurança cibernética

- **Responsabilidade:** um líder de segurança cibernética é fundamental para liderar e coordenar os esforços para proteger os ativos digitais de uma organização, garantindo a implementação de medidas de segurança eficazes e a conformidade com as normas.
- **Visão estratégica:** essa função inclui a identificação de ameaças emergentes, a avaliação de riscos e a adoção de tecnologias e práticas inovadoras para proteção contra ataques cibernéticos.
- **Exemplo e liderança:** os líderes de segurança cibernética estabelecem a cultura de segurança dentro da organização, educando e motivando a equipe a seguir práticas seguras e a estar ciente das possíveis ameaças.



<https://certiprof.com/products/lead-cybersecurity-professional-certificate-lcspc>



...

Módulo 4: Ameaças e vulnerabilidades comuns



CAPC™ Versão 072024



Ameaças e vulnerabilidades comuns

- Identificação e compreensão das principais ameaças
- Reconhecimento de vulnerabilidades em sistemas



Tipos de ameaças

- **Descrição geral:**
 - Vários tipos de ameaças cibernéticas representam riscos para indivíduos e organizações.
 - Compreender essas ameaças é essencial para uma segurança cibernética eficaz.



Malware



- **Definição:**

- Software malicioso projetado para interromper, danificar ou obter acesso não autorizado aos sistemas.



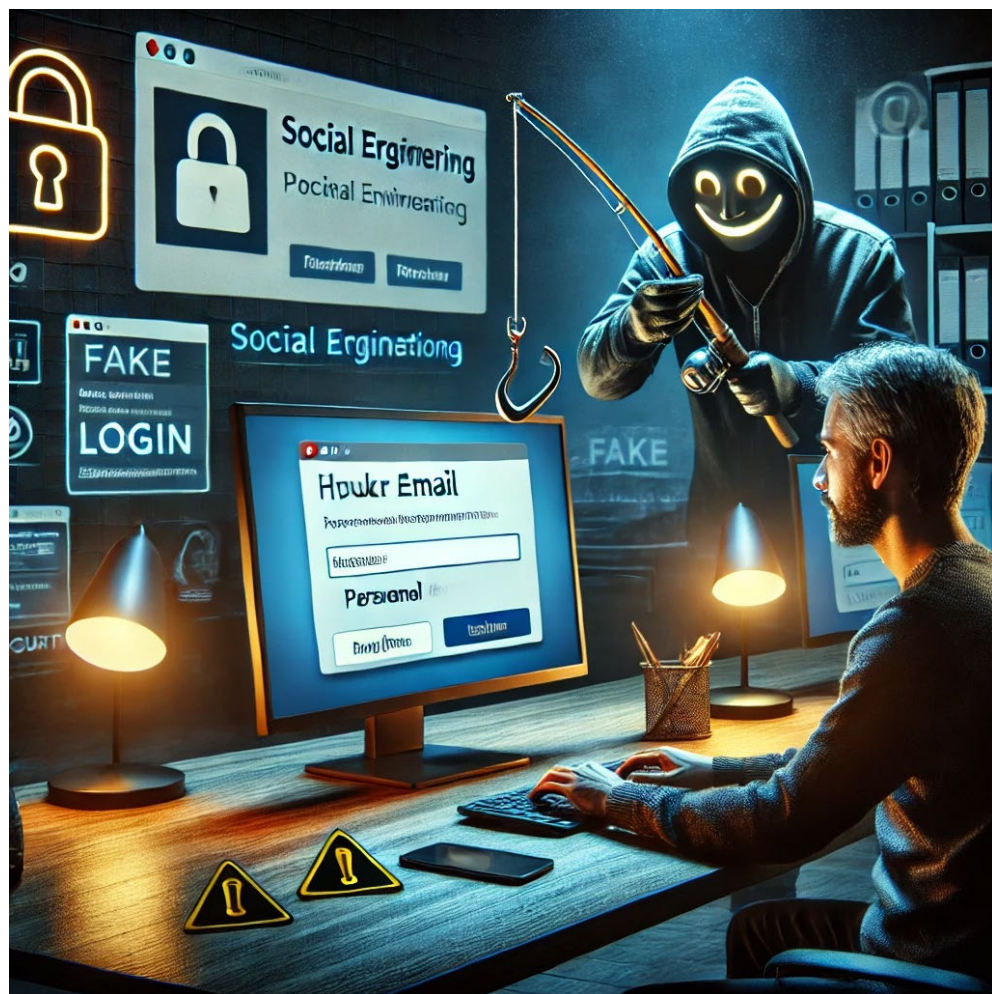
Malware

- **Tipos de malware:**

- Vírus:
 - Função: Anexa-se a arquivos limpos e se espalha pelo sistema.
 - Exemplo: infecção de arquivos ou programas executáveis.
- Worms:
 - Função: Auto-replicação e disseminação sem intervenção humana.
 - Exemplo: Exploração de vulnerabilidades para se espalhar pelas redes.
- Trojans:
 - Função: disfarça-se de software legítimo, mas contém código malicioso.
 - Exemplo: portas traseiras que permitem acesso não autorizado.
- Ransomware:
 - Função: Criptografa dados e exige um resgate para a descriptografia.
 - Exemplo: ataque WannaCry.



Ataques de phishing e engenharia social



- **Phishing:**

- Definição: tentativas enganosas de obter informações confidenciais por meio de e-mails ou sites.
- Exemplos: E-mails falsos de fontes confiáveis, sites fraudulentos que imitam sites legítimos.
- Tipos:
 - **Spear Phishing:** ataques direcionados a indivíduos ou organizações específicas.
 - **Whaling:** Destinado a indivíduos de alto perfil, como executivos.

Ataques de phishing e engenharia social

- **Engenharia social:**

- Definição: manipular as pessoas para que divulguem informações confidenciais.
- Técnicas:
 - **Pretexto:** criação de um cenário fabricado para obter informações.
 - **Isca:** oferecer algo atraente para obter acesso a informações.
 - **Tailgating:** obter acesso não autorizado seguindo pessoas autorizadas.



Ataques de negação de serviço (DoS) e de negação de serviço distribuída (DDoS)

Aumento das ameaças:

- Definição: sobrecarregar um sistema com tráfego para torná-lo inacessível.
- Impacto: Interrupção de serviços e possíveis perdas financeiras.
- Exemplo: saturar um servidor com solicitações para esgotar os recursos.

Ataques DDoS:

- Definição: uso de vários dispositivos comprometidos para lançar um ataque DoS coordenado.
- Impacto: escala maior e mais difícil de mitigar.
- Exemplo: Botnets usados para gerar tráfego maciço para sistemas direcionados.

Estratégias de mitigação:

- Prevenção: implemente firewalls, sistemas de detecção de intrusão e limitação de taxa.
- Resposta: tenha um plano de resposta e use serviços de proteção contra DDoS.



Expansão das principais ameaças

- **Proteção contra malware:**
 - Prática recomendada: atualize regularmente o software, use software antivírus e instrua os usuários.
 - **Ferramentas:** software antivírus, firewalls e plataformas de proteção de endpoints.
- **Prevenção de phishing:**
 - Práticas recomendadas: educação do usuário, filtragem de e-mail e autenticação multifator (MFA).
 - **Ferramentas:** soluções de segurança de e-mail e software antiphishing.
- **Mitigação de DDoS:**
 - Práticas recomendadas: Redundância, balanceamento de carga e serviços de mitigação de DDoS.
 - **Ferramentas:** proteção contra DDoS baseada em nuvem e ferramentas de análise de tráfego.

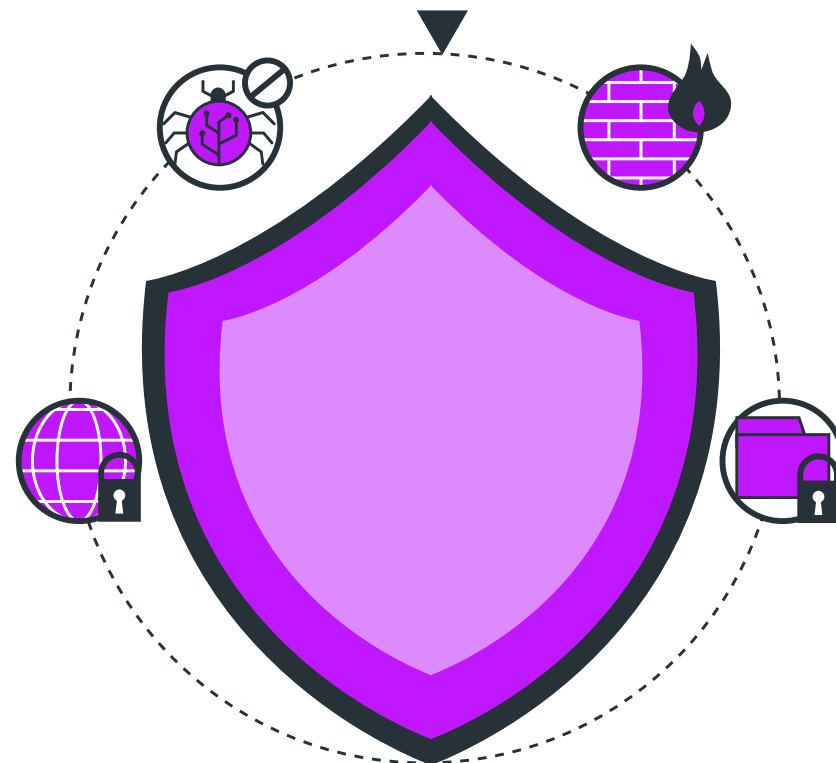


Módulo 5: Vulnerabilidades comuns



Vulnerabilidades comuns

- Identificação de vulnerabilidades em sistemas
- Compreensão do impacto de diversas vulnerabilidades



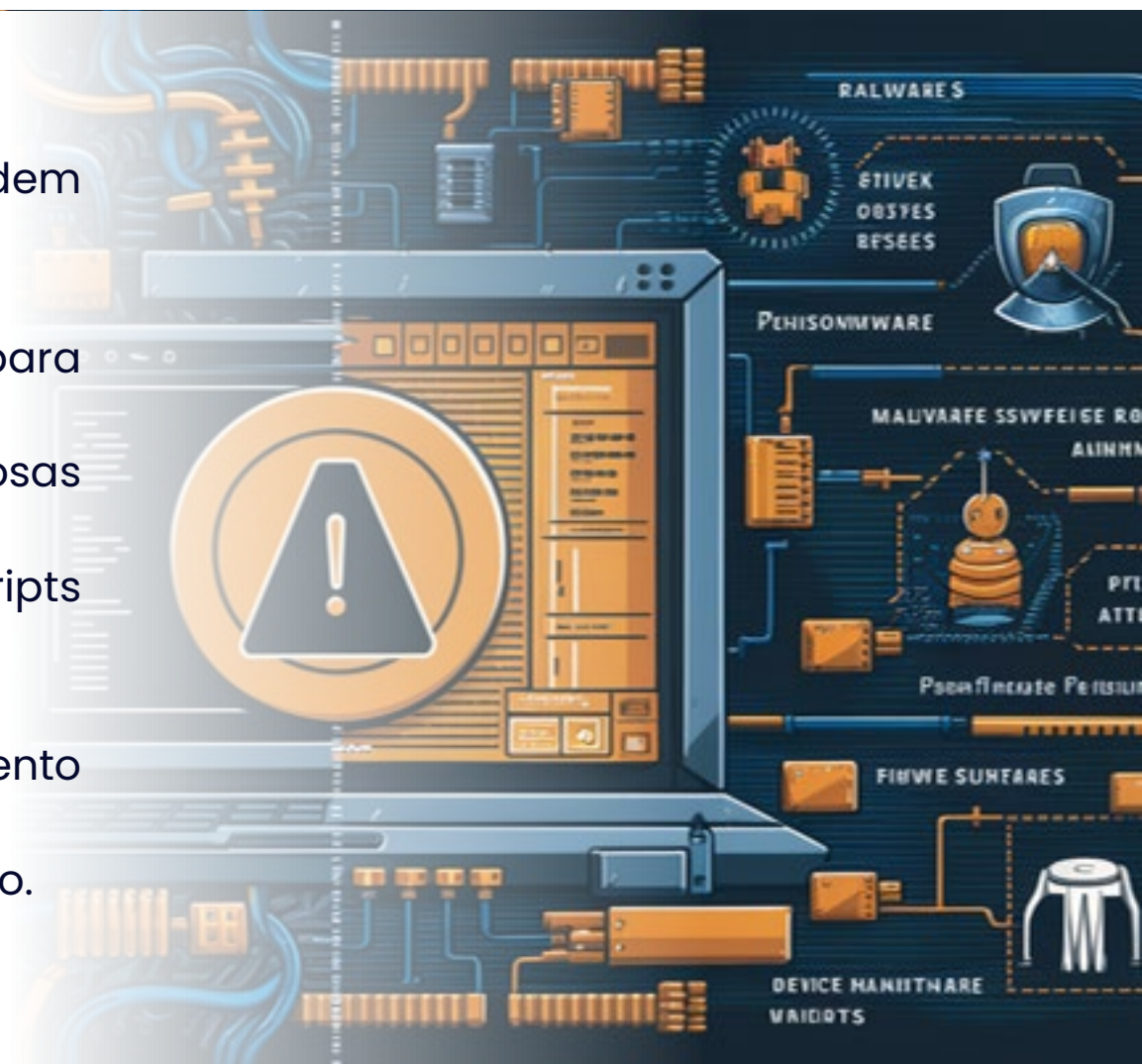
Vulnerabilidades de software e hardware

- **Vulnerabilidades de software:**

- Definição: falhas ou pontos fracos do software que podem ser explorados por invasores.
- Exemplos:
 - Estouro de buffer: ultrapassa o limite do buffer para sobrescrever a memória adjacente.
 - Injeção de SQL: Injeção de consultas SQL maliciosas por meio de campos de entrada.
 - Cross-Site Scripting (XSS): injeção de scripts maliciosos em aplicativos da Web.

- **Mitigação:**

- Atualizações regulares de software e gerenciamento de patches.
- Práticas de codificação segura e revisões de código.
- Uso de Firewalls de Aplicativos da Web (WAF).



Vulnerabilidades de software e hardware



- **Vulnerabilidades de hardware:**
 - Definição: falhas ou pontos fracos em componentes de hardware que podem ser explorados.
 - Exemplos:
 - Meltdown e Spectre: Exploração de falhas no design da CPU para acessar dados confidenciais.
 - Vulnerabilidades de firmware: falhas no firmware que podem ser exploradas para obter controle sobre o hardware.
 - Mitigação:
 - Mantenha o firmware atualizado.
 - Implementar módulos de segurança de hardware (HSM).
 - Use hardware com recursos de segurança incorporados.



Problemas de configuração

- **Configurações incorretas:**
 - Definição: configurações ou definições incorretas que enfraquecem a segurança.
 - Exemplos:
 - Senhas padrão: use senhas padrão que sejam fáceis de adivinhar.
 - APIs não seguras: exposição de APIs sem medidas de segurança adequadas.
 - Portas abertas: deixar portas desnecessárias abertas, tornando-as suscetíveis a ataques.
 - Mitigação:
 - Auditorias regulares de configuração.
 - Use ferramentas automatizadas para verificar configurações incorretas.
 - Siga as práticas recomendadas para configurações seguras.



Problemas de configuração



- **Gerenciamento de configuração:**

- Importância: certifique-se de que todos os sistemas e aplicativos estejam configurados de forma segura.
- Práticas recomendadas:
 - Manter um inventário de todas as configurações.
 - Implementar ferramentas de gerenciamento de configuração.
 - Revise e atualize as configurações regularmente.



Erros humanos e seu impacto na segurança

Erros humanos comuns:

- Suscetibilidade a phishing: ser vítima de golpes de phishing devido à falta de conscientização.
- Senhas fracas: use senhas fáceis de adivinhar ou reutilize-as em várias contas.
- Exposição involuntária de dados: Compartilhamento accidental de informações confidenciais.

Impacto na segurança:

- Incidentes de violação: Erros humanos podem levar a violações de dados e incidentes de segurança significativos.
- Perdas financeiras: custos associados à mitigação de violações causadas por erro humano.
- Danos à reputação: perda de confiança e credibilidade devido a incidentes de segurança.

Mitigação:

- Treinamento e conscientização: programas regulares de treinamento e conscientização sobre segurança cibernética para os funcionários.
- Políticas rígidas: implemente e aplique políticas de segurança rígidas.
- Automação: use ferramentas automatizadas para minimizar o risco de erro humano.



Expansão das principais vulnerabilidades

- **Gerenciamento de vulnerabilidades:**
 - Prática recomendada: avaliações regulares de vulnerabilidade e testes de penetração.
 - **Ferramentas:** Scanners de vulnerabilidade e sistemas de gerenciamento de eventos e informações de segurança (SIEM).
- **Segurança de configuração:**
 - Prática recomendada: siga os padrões e as diretrizes do setor para configurações seguras.
 - **Ferramentas:** ferramentas de gerenciamento de configuração e linhas de base de segurança.
- **Redução de erros humanos:**
 - Prática recomendada: educação e conscientização contínuas, implementação de uma cultura de segurança em primeiro lugar.
 - **Ferramentas:** plataformas de simulação de phishing e análise do comportamento do usuário.



Módulo 6: Medidas de proteção e práticas recomendadas



Medidas de proteção e práticas recomendadas



- **Implementação de estratégias de segurança eficazes**



- **Garantia de uma proteção abrangente**



Proteção de dispositivos e redes



- Proteção da segurança de dispositivos e redes
- Principais estratégias para uma proteção eficaz



Uso de software antivírus e de segurança

Software antivírus:

- Função: Detecta, impede e remove malware.
- Prática recomendada: atualize regularmente o software antivírus, faça varreduras frequentes e use software de boa reputação.

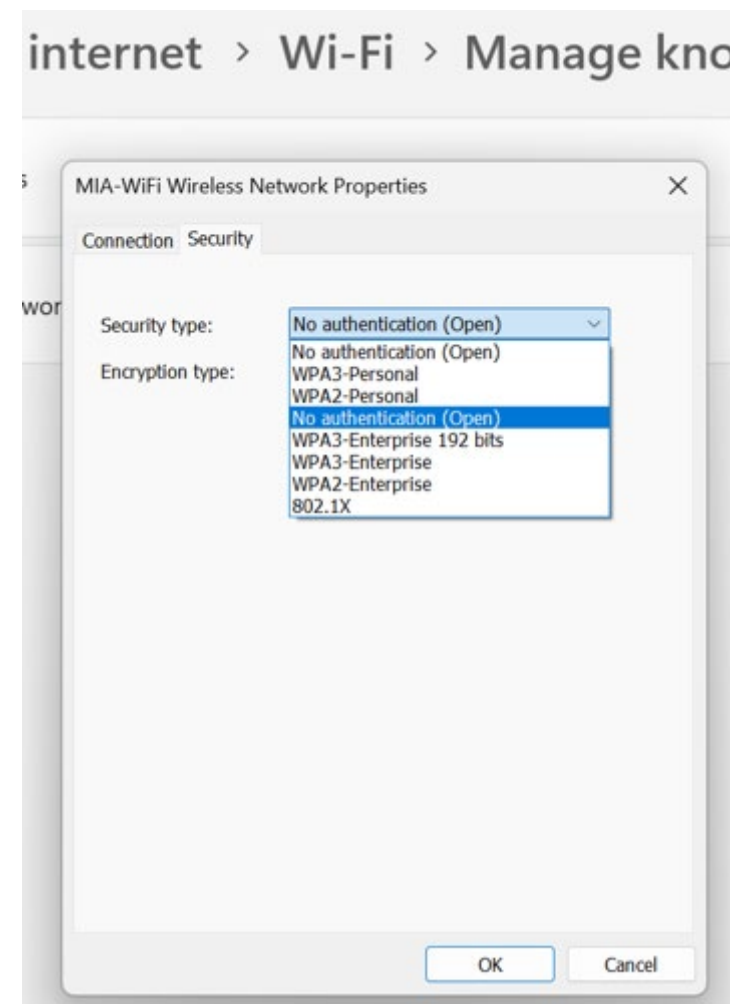
Software de segurança:

- Tipos:
 - Firewalls: monitoram e controlam o tráfego de entrada e saída da rede.
 - Sistemas de detecção de intrusão (IDS): detectam acesso não autorizado ou anomalias.
 - Implementação: combinação de várias ferramentas de segurança para proteção em camadas.



Configuração de rede Wi-Fi segura

- **Configuração básica:**
 - **SSID:** Altere o SSID padrão para algo exclusivo.
 - **Criptografia:** use a criptografia WPA3 para obter segurança máxima.
 - **Senhas:** use senhas fortes e exclusivas para acessar o Wi-Fi.
- **Configurações avançadas:**
 - **Segmentação de rede:** separe as redes de convidados das redes principais.
 - **SSID Hidden (Oculto):** Opcionalmente, oculte o SSID da visualização pública.
 - **Filtragem de MAC:** permite que apenas dispositivos conhecidos se conectem.



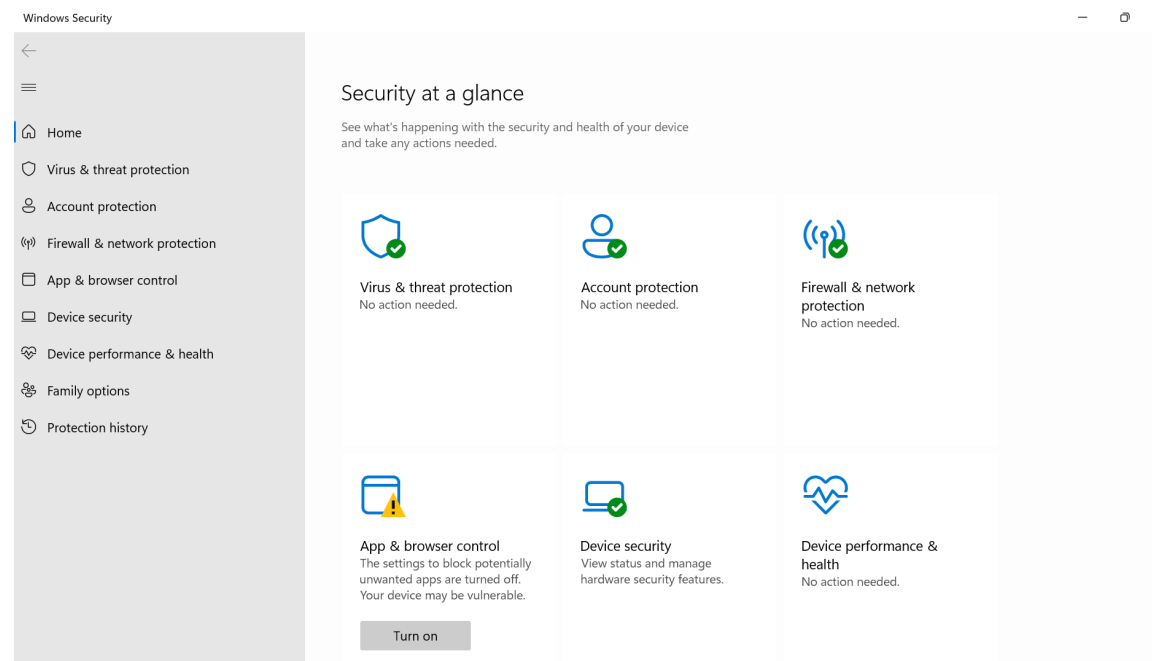
Importância das atualizações e patches de segurança

- **Atualizações de software:**

- Definição: atualizar regularmente o software para as versões mais recentes.
- Objetivo: corrigir vulnerabilidades, adicionar novos recursos e melhorar o desempenho.

- **Patches de segurança:**

- Definição: patches projetados especificamente para corrigir vulnerabilidades de segurança.
- Prática recomendada: habilite as atualizações automáticas, verifique regularmente se há patches e aplique-os imediatamente.

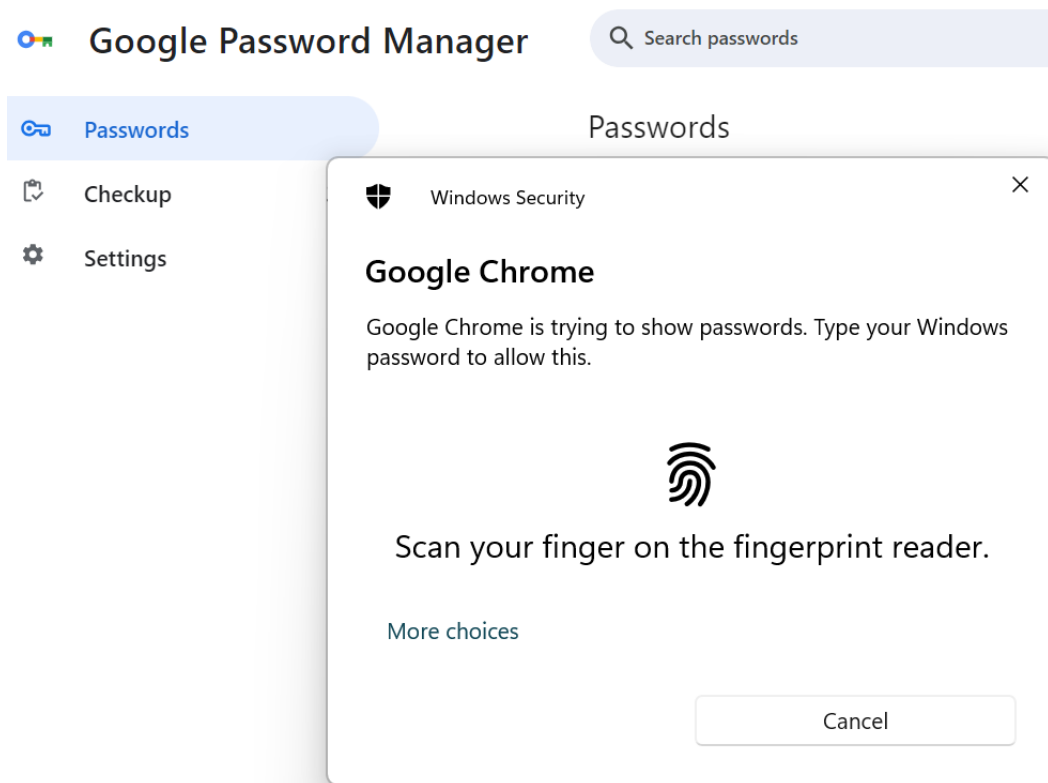


Segurança de informações pessoais e profissionais

- Proteção de informações confidenciais em contextos pessoais e profissionais
- Principais práticas de garantia da informação



Criação e gerenciamento de senhas fortes



- **Senhas fortes:**
 - Características: Longos, complexos e exclusivos para cada conta.
 - Exemplos: Use uma combinação de letras, números e caracteres especiais.
- **Gerenciamento de senhas:**
 - Ferramentas: use gerenciadores de senhas para gerar e armazenar senhas com segurança.
 - Práticas: Evite usar a mesma senha para várias contas e atualize as senhas regularmente.



Uso de autenticação multifatorial (MFA)

Definição:

- **MFA:** requer dois ou mais fatores de verificação para obter acesso.
- **Exemplos:** Senha mais um código enviado para um dispositivo móvel, biometria.

Benefícios:

- **Segurança:** adiciona uma camada extra de proteção, mesmo que um fator seja comprometido.
- **Implementação:** habilite a MFA em todas as contas e sistemas essenciais.



Gerenciamento seguro de e-mails e anexos



- **Segurança do correio eletrônico:**
 - Prática recomendada: Desconfie de e-mails não solicitados, verifique as informações do remetente e evite clicar em links suspeitos.
- **Segurança de anexos:**
 - Diretrizes: não abra anexos de fontes desconhecidas, use antivírus para verificar os anexos e ative a filtragem de e-mail.



Navegação segura na Internet



- Garantia de atividades on-line seguras
- Práticas recomendadas para uma navegação segura



Identificação de sites seguros

- **Indicadores de sites seguros:**
 - HTTPS: certifique-se de que o URL do site comece com "https://".
 - Ícone de cadeado: procure o ícone de cadeado na barra de endereços.
- **Certificados:**
 - Certificados SSL/TLS: verifique a validade do certificado de segurança do site.



Prevenção de fraudes on-line

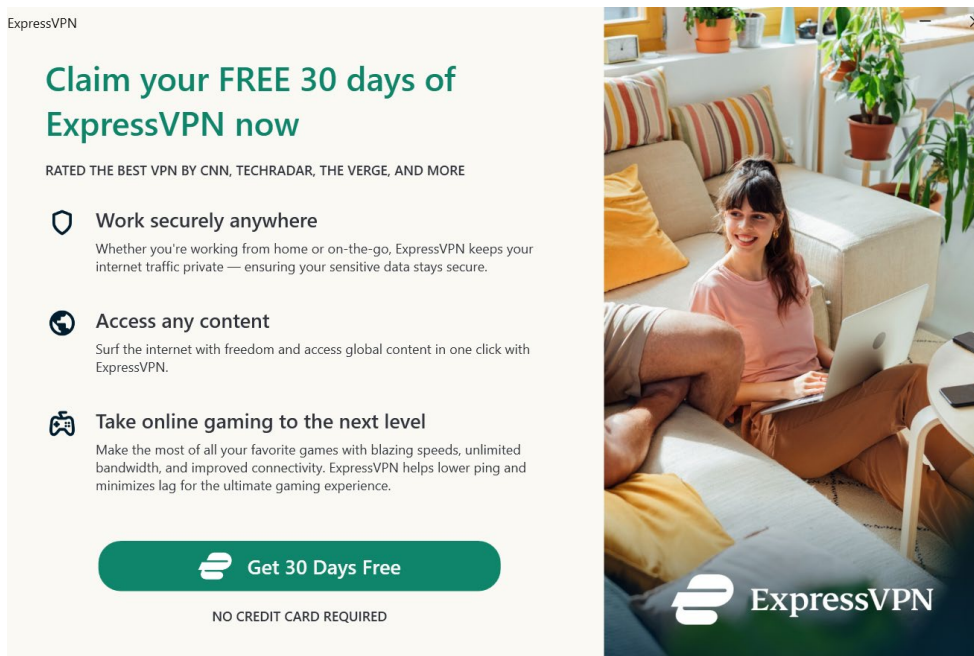


- **Práticas recomendadas:**

- Seja cético: Desconfie de ofertas que sejam boas demais para ser verdade.
- Verifique as fontes: Verifique a autenticidade de sites e e-mails.
- Informações pessoais: não compartilhe informações pessoais ou financeiras em sites não confiáveis.

Uso de VPNs e outras ferramentas de privacidade

- **VPNs (redes privadas virtuais):**
 - Função: Criptografa a conexão com a Internet e oculta o endereço IP.
 - Benefícios: Oferece acesso seguro a dados confidenciais e protege a privacidade.



ExpressVPN

Claim your FREE 30 days of ExpressVPN now

RATED THE BEST VPN BY CNN, TECHRADAR, THE VERGE, AND MORE

- Work securely anywhere**
Whether you're working from home or on-the-go, ExpressVPN keeps your internet traffic private — ensuring your sensitive data stays secure.
- Access any content**
Surf the internet with freedom and access global content in one click with ExpressVPN.
- Take online gaming to the next level**
Make the most of all your favorite games with blazing speeds, unlimited bandwidth, and improved connectivity. ExpressVPN helps lower ping and minimizes lag for the ultimate gaming experience.

 **Get 30 Days Free**

NO CREDIT CARD REQUIRED

 **ExpressVPN**

Add a VPN connection

VPN provider
Windows (built-in) ▾

Connection name

Server name or address

VPN type
Automatic ▾

Type of sign-in info
Username and password ▾

Username (optional)

Password (optional)



Uso de VPNs e outras ferramentas de privacidade

- **Outras ferramentas de privacidade:**
 - Bloqueadores de anúncios: evitam o rastreamento de anúncios.
 - Extensões de navegador: use extensões de navegador voltadas para a privacidade para aumentar a segurança.



...

Módulo 7: Resposta a incidentes e práticas recomendadas



Resposta a incidentes e práticas recomendadas



- Gerenciamento eficaz de incidentes de segurança
- Criação de uma cultura de segurança proativa



Detecção e resposta a incidentes

- Principais etapas para identificar e gerenciar incidentes de segurança
- Garantia de uma resposta rápida e eficaz



Security Incident Management Framework



O que fazer no caso de um incidente de segurança

- **Etapas iniciais:**

- Identificação: Reconhecer os sinais de um incidente de segurança.
- Contenção: Limitar o impacto do incidente isolando os sistemas afetados.

- **Ações imediatas:**

- Notificar: Informar as partes interessadas relevantes e a equipe de resposta a incidentes.
- Preservar evidências: certifique-se de que todos os registros e dados relacionados ao incidente sejam preservados.

- **Comunicação:**

- Comunicação interna: mantenha a equipe de resposta a incidentes e as principais partes interessadas informadas.
- Comunicação externa: preparar declarações para clientes, parceiros e o público, se necessário.



Protocolos de resposta e recuperação

- **Plano de resposta a incidentes:**
 - Preparação: desenvolva e atualize regularmente um plano de resposta a incidentes.
 - Fases da resposta: Siga uma abordagem estruturada: Preparação, Identificação, Contenção, Erradicação, Recuperação e Lições Aprendidas.
- **Etapas de recuperação:**
 - Erradicação: Eliminar a causa do incidente (por exemplo, malware).
 - Restaurar: restaurar os sistemas para a operação normal.
 - Validação: verificar se os sistemas estão seguros e funcionando corretamente.
- **Ações pós-incidente:**
 - Revisão: Analise o incidente para entender o que aconteceu e por quê.
 - Aprimoramento: atualizar as medidas de segurança e os planos de resposta com base nas lições aprendidas.



Importância da documentação e do relatório de incidentes

- **Documentação:**

- Detalhes: Registre todas as ações tomadas durante a resposta ao incidente.
- Registros: mantenha registros detalhados das comunicações, decisões e ações.
- Evidência: preservação de evidências para possível análise legal ou forense.

- **Relatórios de incidentes:**

- Relatórios internos: assegure-se de que os incidentes sejam relatados dentro da organização de acordo com o protocolo.
- Requisitos regulamentares: Cumprir os requisitos legais e regulamentares de relatórios.
- Lições aprendidas: use os relatórios para melhorar a resposta a incidentes e as medidas de segurança.



Aumento da conscientização e treinamento contínuo

- Desenvolvimento de uma organização com consciência de segurança
- Principais estratégias para treinamento contínuo e conscientização



Criação de uma cultura de segurança na organização

- **Compromisso de liderança:**
 - Abordagem de cima para baixo: garantir que a liderança priorize e promova a segurança cibernética.
 - Recursos: alocar recursos para iniciativas de segurança cibernética.
- **Envolvimento dos funcionários:**
 - Responsabilidade: Incentive todos os funcionários a assumirem a responsabilidade pela segurança.
 - Compromisso: promover uma cultura de abertura e compromisso com as questões de segurança.
- **Conformidade com a política:**
 - Políticas claras: desenvolva políticas de segurança claras e aplique-as de forma consistente.
 - Responsabilidade: responsabilizar os indivíduos por seguir as práticas de segurança.



Programas contínuos de conscientização e treinamento

- **Treinamento regular:**

- Frequência: realize sessões regulares de treinamento sobre segurança cibernética.
- Tópicos: Cobrindo ameaças atuais, práticas recomendadas e protocolos de resposta.

- **Campanhas de conscientização:**

- Métodos: use e-mails, pôsteres e reuniões para aumentar a conscientização.
- Foco: destacar ameaças comuns, como phishing e engenharia social.

- **Simulações de ataque:**

- Simulações de phishing: realize testes regulares de phishing para instruir os funcionários.
- Exercícios: realize exercícios de resposta a incidentes para garantir a preparação.



Recursos adicionais e próximas etapas

Recursos:

- Diretrizes: forneça aos funcionários acesso a diretrizes e recursos de segurança cibernética.
- Ferramentas: ofereça ferramentas como gerenciadores de senhas e software antivírus.

Próximas etapas:

- Melhoria contínua: atualize regularmente os materiais de treinamento e as medidas de segurança.
- Feedback: incentive o feedback para aprimorar os programas de treinamento.
- Manter-se informado: esteja ciente das últimas tendências e ameaças à segurança cibernética.



Certificação de auditor líder ISO 27001

O que é a ISO 27001

A ISO 27001 é uma norma internacional que especifica os requisitos para um sistema de gerenciamento de segurança da informação (ISMS). Ela fornece uma estrutura para gerenciar a segurança dos ativos de informação, garantindo sua confidencialidade, integridade e disponibilidade.

Importância da função de auditor líder de segurança da ISO 27001

- **Responsabilidade e verificação:** O auditor líder de segurança da ISO 27001 tem a responsabilidade de avaliar e verificar se a organização atende aos requisitos da norma ISO 27001. Isso inclui a análise das políticas, procedimentos e controles de segurança implementados.
- **Identificação de melhorias:** essa função é fundamental para identificar áreas de melhoria contínua no sistema de gerenciamento de segurança da informação. Os auditores líderes ajudam as organizações a fortalecer suas defesas contra ameaças e a manter a eficácia de seus controles de segurança.
- **Conformidade e confiança:** os auditores líderes garantem que as organizações mantenham a conformidade com os padrões internacionais e legais, o que aumenta a confiança dos clientes, parceiros e partes interessadas na capacidade da organização de proteger seus dados e gerenciar os riscos de segurança.



<https://certiprof.com/products/certified-iso-iec-27001-lead-auditor-i27001la?variant=43740096626942>



Módulo 8: Política e conformidade



Política e conformidade



- Entendendo o papel da política e da regulamentação na segurança cibernética
- Garantia de conformidade com os padrões legais e do setor



Políticas de segurança



- Estabelecimento de uma estrutura para a segurança organizacional
- Principais tipos de políticas de segurança



Desenvolvimento e implementação de políticas de segurança

- **Desenvolvimento de políticas:**
 - Avaliação: Identificar riscos e requisitos.
 - Estabelecimento: Desenvolver políticas adaptadas às necessidades da organização.
 - Revisão: revise e atualize regularmente as políticas.
- **Implementação:**
 - Comunicação: assegure-se de que todos os funcionários estejam cientes das políticas.
 - Treinamento: Forneça treinamento sobre a adesão à política.
 - Aplicação: implemente mecanismos para aplicar políticas.
- **Exemplos:**
 - Políticas de senha: diretrizes para criar e gerenciar senhas.
 - Políticas de resposta a incidentes: Etapas a serem tomadas no caso de um incidente de segurança.



Política de uso aceitável (AUP)

- **Definição:**

- PUA: regras que definem o uso aceitável e inaceitável dos recursos organizacionais.

- **Componentes:**

- Escopo: quais recursos são cobertos (por exemplo, Internet, e-mail, dispositivos).
- Responsabilidades do usuário: expectativas sobre o comportamento do usuário.
- Ações proibidas: atividades que não são permitidas (por exemplo, downloads ilegais, acesso a sites inadequados).

- **Implementação:**

- Acordo: Exigir que os funcionários leiam e assinem a PUA.
- Conformidade: monitore a conformidade e aplique as consequências das violações.



Políticas de acesso à informação

- **Objetivo:**

- Controle: defina quem tem acesso a quais informações e por quê.
- Proteção: assegure-se de que as informações confidenciais sejam acessíveis somente ao pessoal autorizado.

- **Componentes:**

- Níveis de acesso: defina diferentes níveis de acesso com base nas funções.
- Autorização: processo de concessão e revogação de acesso.
- Monitoramento: analise regularmente os registros de acesso para detectar acessos não autorizados.

- **Exemplos:**

- Controle de acesso baseado em função (RBAC): atribua acesso com base em funções de trabalho.
- Princípio do menor privilégio: os usuários recebem o mínimo de acesso necessário para realizar seu trabalho.



Conformidade regulatória

- Garantir a adesão às leis e normas de segurança cibernética
- Principais estruturas regulatórias e requisitos de conformidade



Introdução à legislação e regulamentação da segurança cibernética

- **Descrição geral:**
 - Objetivo: proteger a privacidade e a segurança dos dados.
 - Escopo: aplica-se a vários setores e tipos de dados.
- **Principais regulamentos:**
 - **Regulamento Geral sobre a Proteção de Dados (GDPR):**
 - Escopo: aplica-se à proteção de dados e à privacidade na UE.
 - Requisitos: Consentimento para processamento de dados, direito de acesso e notificações de violação de dados.
 - **Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA):**
 - Escopo: aplica-se a dados de saúde nos EUA.
 - Requisitos: Proteger os dados do paciente, garantir a confidencialidade, a integridade e a disponibilidade.



Certificação de proteção de dados

A importância do gerenciamento adequado da proteção de dados em uma organização

- **Conformidade legal:** as organizações devem estar em conformidade com o GDPR para evitar multas e penalidades severas. Isso inclui a obtenção de consentimento explícito para o processamento de dados, a implementação de medidas de segurança robustas e a comunicação de violações de segurança.
- **Confiança do cliente:** O gerenciamento adequado dos dados pessoais ajuda a manter e aumentar a confiança do cliente. As organizações que protegem diligentemente os dados de seus clientes podem se diferenciar positivamente no mercado.
- **Mitigação de riscos:** a implementação das práticas recomendadas pelo GDPR reduz o risco de incidentes de segurança e suas consequências negativas, como perdas financeiras, danos à reputação e litígios legais.



<https://certiprof.com/products/fundamentos-na-lei-geral-de-protecao-de-dados-lgpdf%E2%84%A2>



Introdução à legislação e regulamentação da segurança cibernética

- **Outros regulamentos:**
 - California Consumer Privacy Act (CCPA): lei de privacidade de dados da Califórnia.
 - Federal Information Security Management Act (FISMA): padrões federais de segurança de dados.



Conformidade com padrões como GDPR, HIPAA, etc.

- **Conformidade com o GDPR:**
 - Mapeamento de dados: identifique onde os dados pessoais são armazenados e processados.
 - Consentimento: obtenha e documente o consentimento do usuário.
 - Direitos dos titulares dos dados: implemente mecanismos para lidar com solicitações de acesso e exclusão de dados.
- **Conformidade com a HIPAA:**
 - Avaliação de riscos: realize avaliações regulares de riscos.
 - Políticas e procedimentos: Implementar e aplicar políticas de segurança.
 - Treinamento: forneça treinamento regular de conformidade com a HIPAA.
- **Etapas comuns para a conformidade:**
 - Análise de lacunas: identifique as áreas em que as práticas atuais não atendem aos requisitos regulamentares.
 - Implementação: desenvolva e implemente as políticas e os controles necessários.
 - Monitoramento: monitore e audite continuamente os esforços de conformidade.



Auditorias e controles de segurança



- **Objetivo:**
 - Verificação: garantir a conformidade com as políticas e normas de segurança.
 - Aprimoramento: identifique e resolva os pontos fracos da segurança.
- **Tipos de auditorias:**
 - Auditorias internas: conduzidas pela equipe interna para avaliar a conformidade e identificar problemas.
 - Auditorias externas: Realizadas por auditores externos para uma análise imparcial.



Auditorias e controles de segurança



- **Processo de auditoria:**

- Preparação: Defina o escopo e os objetivos.
- Implementação: realize auditorias por meio de entrevistas e análises de documentos para detectar e tratar o acesso não autorizado.
- Relatórios: documentar os resultados e fazer recomendações.

- **Controles:**

- Controles preventivos: medidas para evitar incidentes de segurança (por exemplo, firewalls, controles de acesso).
- Controles de detecção: medidas para detectar incidentes (por exemplo, sistemas de detecção de intrusão).
- Controles corretivos: medidas para corrigir e se recuperar de incidentes (por exemplo, backups, planos de resposta a incidentes).



Certificação de auditor interno ISO 27001

Importância da função do auditor interno na segurança ISO 27001

- **Responsabilidade pela avaliação:** O auditor interno de segurança da ISO 27001 é responsável por avaliar e garantir que a organização esteja em conformidade com os requisitos da norma ISO 27001. Isso envolve a realização de auditorias internas periódicas para identificar áreas de melhoria e garantir a conformidade contínua.
- **Melhoria contínua:** essa função é fundamental para identificar e solucionar os pontos fracos do sistema de gerenciamento de segurança da informação. Os auditores internos fornecem recomendações valiosas para melhorar continuamente as práticas de segurança e minimizar os riscos.
- **Confiança e conformidade:** ter auditores internos treinados e certificados na ISO 27001 ajuda a manter a confiança dos clientes e parceiros de negócios, garantindo que a organização esteja em conformidade com os padrões internacionais e as regulamentações legais, o que é fundamental para proteger informações confidenciais e manter a reputação da organização.



<https://certiprof.com/products/certified-iso-iec-27001-auditor-i27001a?variant=32820759593059>



...

Módulo 9: Segurança cibernética no ambiente de negócios



CAPC™ Versão 072024



Segurança cibernética no ambiente de negócios



- Implementação de práticas eficazes de segurança cibernética nas organizações
- Abordagem dos desafios específicos dos ambientes corporativos

Segurança no trabalho remoto



- Garantia de segurança em ambientes de trabalho remoto
- Principais estratégias e práticas recomendadas



Boas práticas para o trabalho remoto seguro

- **Segurança do equipamento:**
 - Software antivírus e de segurança: certifique-se de que todos os dispositivos tenham um software de segurança atualizado.
 - Atualizações frequentes: Mantenha os sistemas operacionais e aplicativos atualizados.
 - Criptografia: use criptografia para dados e comunicações confidenciais.
- **Segurança de rede:**
 - Wi-Fi seguro: use senhas fortes e criptografia WPA3 para redes domésticas.
 - VPN: use redes privadas virtuais (VPN) para proteger as conexões com a Internet.
- **Práticas do usuário:**
 - Conscientização sobre phishing: treine seus funcionários para reconhecer e evitar golpes de phishing.
 - Senhas fortes: use senhas completas e evite reutilizá-las.
 - Autenticação multifatorial (MFA): habilite a MFA para todas as contas críticas.



Uso de dispositivos pessoais e BYOD

- **Políticas de BYOD:**

- Instruções claras: desenvolva e aplique políticas para o uso de dispositivos pessoais no trabalho.
- Equipamentos permitidos: mantenha uma lista de dispositivos e sistemas operacionais permitidos.
- Requisitos de segurança: certifique-se de que os dispositivos pessoais estejam em conformidade com os padrões de segurança (por exemplo, antivírus, criptografia).

- **Proteção de dados:**

- Segregação: mantenha os dados pessoais e de trabalho separados nos dispositivos pessoais.
- Limpeza remota: implemente funções de limpeza remota para dispositivos perdidos ou roubados.
- Controles de acesso: restrinja o acesso a dados confidenciais com base nas funções e nos dispositivos do usuário.



Garantir a segurança da comunicação e da colaboração on-line

- **Ferramentas de comunicação seguras:**
 - Mensagens criptografadas: use ferramentas que ofereçam criptografia de ponta a ponta (por exemplo, Signal, WhatsApp).
 - Videoconferência segura: use plataformas com fortes recursos de segurança (por exemplo, Zoom com criptografia, Microsoft Teams).
- **Ferramentas de colaboração:**
 - Compartilhamento de documentos: Use plataformas seguras de compartilhamento de documentos (por exemplo, Google Drive com controles de acesso apropriados).
 - Controles de acesso: implemente o acesso baseado em funções às ferramentas de colaboração.
- **Boas práticas:**
 - Treinamento regular: Ofereça treinamento contínuo sobre práticas de comunicação segura.
 - Monitoramento: monitore e audite regularmente o uso de ferramentas de comunicação e colaboração.



Segurança cibernética para executivos e líderes

- Compreensão do papel da liderança na segurança cibernética
- Principais responsabilidades e integração estratégica



Responsabilidades dos líderes de segurança cibernética

- **Monitoramento estratégico:**

- Supervisão estratégica: visão e objetivos: defina a visão e os objetivos de segurança cibernética da organização.
- Desenvolvimento de políticas: supervisionar a criação e a implementação de políticas de segurança.
- Alocação de recursos: garanta recursos adequados para iniciativas de segurança cibernética.

- **Gerenciamento de riscos:**

- Gerenciamento de riscos: Avalie regularmente os riscos e as vulnerabilidades da segurança cibernética.
- Estratégias de mitigação: Desenvolver e implementar estratégias para mitigar os riscos identificados.

- **Conformidade:**

- Conformidade normativa: garanta a conformidade com as leis e normas de segurança cibernética relevantes.
- Auditoria e revisão: revise e audite periodicamente as práticas e políticas de segurança.



Integração da segurança cibernética à estratégia de negócios

- **Alinhamento com os objetivos comerciais:**
 - Segurança cibernética como facilitador de negócios: considere a segurança cibernética como um componente do sucesso dos negócios.
 - Planejamento estratégico: integre as considerações de segurança cibernética ao planejamento geral dos negócios.
- **Colaboração interdepartamental:**
 - Coordenação interdepartamental: garantir que as políticas de segurança cibernética sejam implementadas em todos os departamentos.
 - Envolvimento das partes interessadas: envolva as partes interessadas no planejamento e na implementação da segurança cibernética.
- **Melhoria contínua:**
 - Estratégias adaptativas: atualize regularmente as estratégias de segurança cibernética para lidar com as ameaças em evolução.
 - Inovação: Incentivar a adoção de novas tecnologias e abordagens para melhorar a segurança.

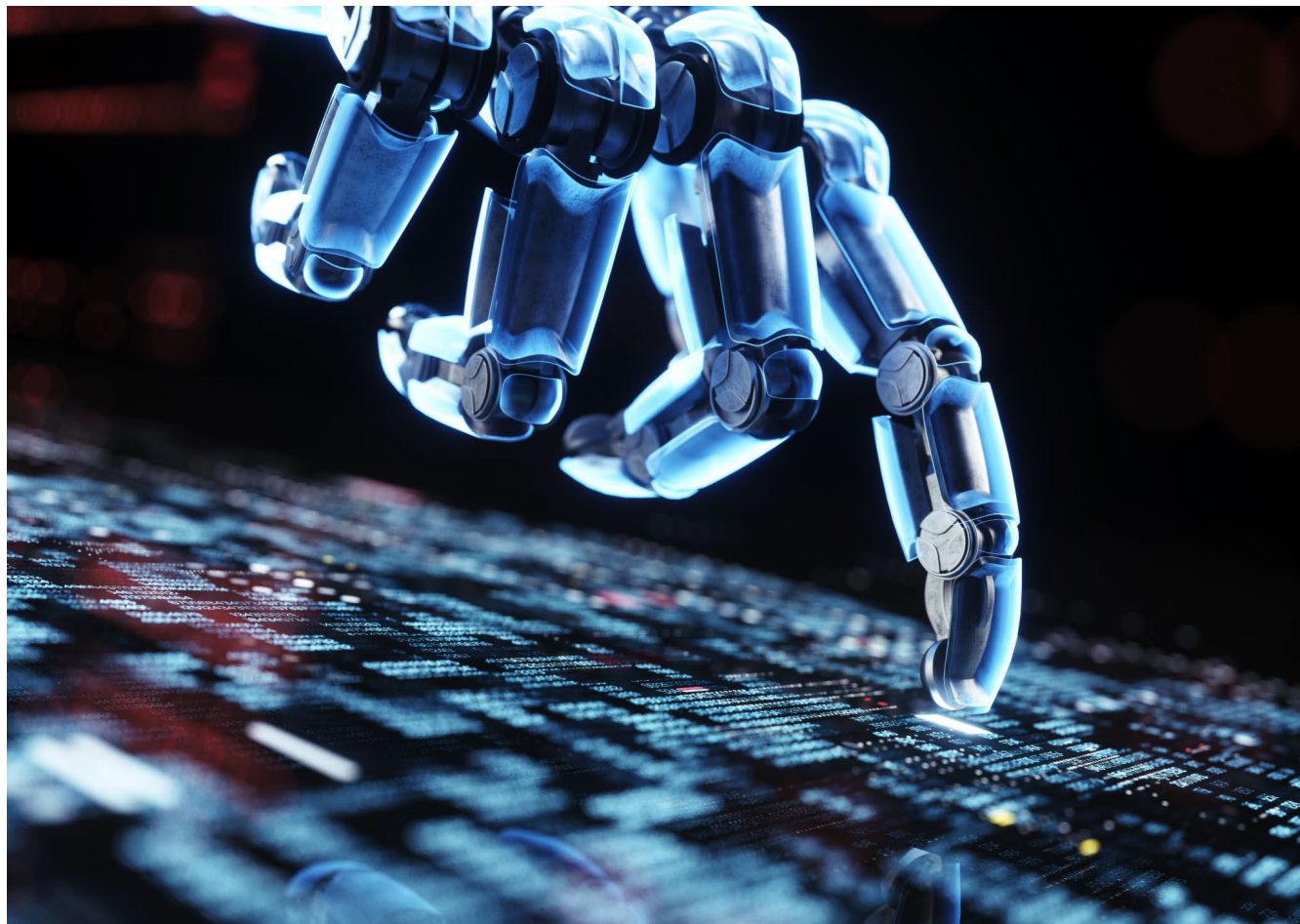


Avaliação de risco e tomada de decisão informada

- **Avaliação de riscos:**
 - Identificar riscos: reconhecer os possíveis riscos de segurança cibernética para a organização.
 - Avaliar o impacto: Avaliar o impacto potencial dos riscos identificados.
 - Priorizar: priorize os riscos de acordo com sua gravidade e probabilidade.
- **Tomada de decisões:**
 - Decisões informadas: baseie as decisões em avaliações de risco completas.
 - Alocação de recursos: alocar recursos para tratar os riscos de maior prioridade.
 - Monitoramento e revisão: monitore continuamente o ambiente de risco e ajuste as estratégias conforme necessário.



Introdução ao gerenciamento de identidade e acesso (IAM)



- Entendendo o IAM e sua importância na segurança cibernética
- Conceitos básicos e terminologia



Conceitos básicos de AMI

- **Gerenciamento de identidade:**
 - Definição: O processo de identificação de indivíduos em um sistema e o controle de seu acesso aos recursos.
 - Componentes: Identities de usuário, autenticação e autorização.
- **Gerenciamento de acesso:**
 - Definição: garantir que as pessoas certas tenham acesso aos recursos certos no momento certo.
 - Princípios: Menor privilégio, controle de acesso baseado em função (RBAC) e segregação de funções.
- **Autenticação e autorização:**
 - Autenticação: verificação da identidade de um usuário (por exemplo, senhas, biometria).
 - Autorização: concessão ou negação de acesso a recursos com base nas permissões do usuário.



Ferramentas e tecnologias de IAM

- **Ferramentas:**

- Single Sign-On (SSO): permite que os usuários se autentiquem uma vez e acessem vários sistemas.
- Autenticação multifatorial (MFA): requer várias formas de verificação.
- Identity Governance and Administration (IGA): gerencia as identidades dos usuários e as permissões de acesso.

- **Tecnologias:**

- Serviços de diretório: bancos de dados centralizados que armazenam informações do usuário (por exemplo, Active Directory).
- Serviços de federação: permitem o logon único em diferentes domínios (por exemplo, SAML, OAuth).
- Plataformas de gerenciamento de acesso: plataformas de ponta a ponta que gerenciam identidades e acesso (por exemplo, Okta, Ping Identity).



Boas práticas para o gerenciamento de identidade e acesso

- **Gerenciamento do ciclo de vida da identidade:**
 - Integração: garanta a criação e a atribuição corretas de identidades de usuários.
 - Baixo: desabilite rapidamente o acesso de funcionários que estão saindo.
 - Revisões periódicas: realize revisões periódicas do acesso para garantir níveis adequados de acesso.
- **Controles de acesso:**
 - Controle de acesso baseado em função (RBAC): atribua acesso com base nas funções do cargo.
 - Mínimo privilégio: concede aos usuários o acesso mínimo necessário para suas funções.
- **Monitoramento e auditoria:**
 - Logs de atividade: mantenha registros da atividade e do acesso do usuário.
 - Auditorias regulares: realize auditorias regulares para detectar e lidar com o acesso não autorizado.





Siga-nos, entre em contato!



www.certiprof.com

CERTIPROF® is a registered trademark of Certiprof,
LLC in the United States and/or other countries.