

Módulo 1 - Aulas 1 e 2

Módulo 1: Princípios de Segurança e Engenharia Social

Aula 1: Princípios de Segurança da Informação

Objetivos

- ☒ Internalizar os conceitos básicos de segurança da informação e tríade CID.
- ☒ Compreender a relação entre risco, vulnerabilidade e ameaça.
- ☒ Conhecer e explorar as principais tarefas relacionadas à cybersecurity.

Conceitos

- ☒ Tríade CID.
- ☒ Vulnerabilidade, ameaça e risco.
- ☒ Framework de segurança da informação.

Introdução

A segurança da informação é um tema de relevância inegável na sociedade moderna. Em um mundo cada vez mais digital e interconectado, a proteção dos dados e informações tornou-se uma preocupação crítica para organizações e indivíduos. Nossa vida cotidiana está intrinsecamente ligada ao compartilhamento de informações por meio da internet, desde a troca de mensagens pessoais até transações financeiras e operações comerciais complexas.

Para garantir a integridade, confidencialidade e disponibilidade dessas informações como profissional, a compreensão dos princípios fundamentais da segurança da informação é essencial. Neste contexto, a tríade CID (Confidencialidade, Integridade e Disponibilidade) emerge como o alicerce sobre o qual repousam todas as estratégias de proteção e segurança. Esses três princípios interconectados formam a base que sustenta as melhores práticas de segurança, ajudando-nos a entender como proteger ativos digitais contra ameaças potenciais.

Ao longo desta aula, exploraremos os conceitos básicos de segurança da informação, desvendaremos a relação intrincada entre vulnerabilidade, ameaça e risco, e examinaremos o framework de segurança cibernética proposto pelo Instituto Nacional de Padrões e Tecnologia (NIST), que nos oferece diretrizes para a proteção de sistemas e dados digitais.

À medida que nos aprofundamos nesse assunto, vocês estarão mais qualificados para enfrentar os desafios de um mundo digital em constante evolução, onde a segurança da informação é uma prioridade inegociável.

Conceitos básicos de Segurança da Informação

Segurança da Informação

A Segurança da Informação é um campo multidisciplinar que se concentra em proteger os ativos de informação de uma organização contra ameaças e garantir que esses ativos permaneçam confidenciais, íntegros e disponíveis quando necessário. É um conjunto de práticas, políticas, procedimentos e tecnologias projetadas para salvaguardar informações sensíveis e valiosas.

Em outras palavras, a segurança da informação refere-se à proteção de recursos de dados contra acesso não autorizado, modificação não autorizada, ataques, roubos ou destruição. Os dados podem estar vulneráveis devido à forma como são armazenados, a forma como são transferidos ou a forma como são processados. Os sistemas usados para armazenar, transmitir e processar dados devem refletir as propriedades de segurança. A informação segura tem três propriedades, muitas vezes referidas como Tríade da CID: Confidencialidade, Integridade e Disponibilidade.

Preservar a informação é essencial em todos os setores, desde empresas e organizações governamentais até no uso pessoal de dispositivos e contas online. A proteção adequada evita vazamentos de dados, perda de informações confidenciais, interrupções de serviços e outros impactos negativos associados a ameaças de segurança cibernética e física. Portanto, a segurança da informação desempenha um papel vital na proteção da confidencialidade, integridade e disponibilidade dos ativos de informação no mundo digital.



Segurança da Informação.

Tríade CID

A tríade CID é o pilar de sustentação da segurança da informação:

- **Confidencialidade:** garantir que as informações só sejam acessíveis por pessoas autorizadas. Isso significa que os dados não devem ser expostos a

peças não autorizadas. A confidencialidade é frequentemente alcançada por meio de mecanismos de controle de acesso, como senhas, autenticação multifatorial e criptografia.

- **Integridade:** garantir que as informações permaneçam precisas, completas e íntegras protegendo-as contra alterações não autorizadas. Isso envolve a proteção dos dados contra modificações não autorizadas ou corrupção. A integridade é mantida por meio de práticas de controles como assinaturas digitais, verificações de integridade de dados e sistemas de controle de versão.
- **Disponibilidade:** garantir que as informações estejam disponíveis quando necessário. Isso implica que sistemas e dados devem estar acessíveis e funcionais, sem interrupções não planejadas. A disponibilidade é mantida por meio de práticas como planejamento de continuidade de negócios e redundância de sistemas.



Tripé da Segurança.

Outros conceitos aplicados em Segurança da Informação

1. **Não repúdio:** alguns pesquisadores identificam outras propriedades que protegem os sistemas e que deveriam ser mencionadas também. A mais importante é o não repúdio. Significa que um sujeito não pode negar que fez algo, tal como criar, modificar ou enviar um documento. Impedir que uma pessoa negue ter realizado uma ação específica, como enviar uma mensagem ou realizar uma transação. Mecanismos de não repúdio, tal como assinaturas digitais, podem ser usados para garantir a autenticidade das ações.
2. **Autenticidade:** certificar-se de que a origem das informações seja legítima e confiável. Isso envolve a verificação da identidade de usuários e sistemas para evitar a falsificação de informações ou a entrada não autorizada.
3. **Controle de Acesso:** Gerenciar quem tem permissão para acessar informações ou recursos. O controle de acesso define quais usuários ou sistemas podem acessar quais dados e em que condições.
4. **Autenticação e Autorização:** a autenticação envolve verificar a identidade de um usuário antes de conceder acesso a recursos. A autorização determina o que um usuário autenticado pode fazer após o acesso ser concedido.
5. **Princípio do Menor Privilégio:** o princípio do menor privilégio significa que os usuários e sistemas devem ter apenas o acesso necessário para realizar suas tarefas. Isso minimiza o risco de acesso não autorizado.
6. **Gestão de Riscos:** avaliar e mitigar os riscos de segurança associados às informações. Isso envolve a identificação de vulnerabilidades, ameaças potenciais e a implementação de medidas para reduzir esses riscos a níveis aceitáveis.
7. **Ativos de Informação:** ativos de informação são todos os dados e recursos que têm valor para uma organização. Isso pode incluir dados confidenciais, sistemas de computador, documentos físicos, hardware e software.
8. **Ameaças à Segurança da Informação:** as ameaças são eventos ou circunstâncias que podem causar danos aos ativos de informação. Isso pode incluir hackers, malware, desastres naturais, erro humano, entre outros.
9. **Ataques Cibernéticos:** ataques cibernéticos são ações deliberadas para comprometer a segurança da informação. Isso inclui malware, phishing, ataques de negação de serviço (DDoS) e engenharia social.
10. **Criptografia:** a criptografia é uma técnica que transforma informações em um formato ilegível, a menos que o receptor tenha a chave apropriada para decifrá-las. É fundamental para proteger a confidencialidade dos dados.



Pilares da Segurança da Informação.

Relação entre vulnerabilidade, ameaça e risco

Como parte da avaliação e monitoramento da segurança, os times de segurança devem identificar as formas pelas quais seus sistemas podem ser atacados. Essas avaliações envolvem mapear vulnerabilidades, ameaças e riscos. O entendimento dessas relações proporciona a tomada de decisões embasadas por informações sobre a segurança, permitindo que as organizações priorizem seus esforços e aloquem recursos de forma eficaz para proteger ativos críticos e reduzir os riscos a níveis aceitáveis.

Vulnerabilidade

Uma vulnerabilidade é uma fraqueza ou deficiência em um sistema, processo, aplicativo, pessoa ou organização que pode ser acionada acidentalmente ou explorada intencionalmente por uma ameaça para causar danos. As vulnerabilidades podem resultar de falhas de segurança (como o uso de senhas inseguras), configurações inadequadas, falhas de projeto em aplicativos (como não verificar dados de entrada), falta de atualizações de software e correções (patches), uso indevido de softwares ou protocolos de comunicação, arquitetura de rede mal projetada, segurança física inadequada e outros fatores.

Ameaça

Uma ameaça é qualquer evento ou circunstância que tem o potencial de causar danos ou explorar uma vulnerabilidade. É o potencial de alguém ou alguma coisa explorar uma vulnerabilidade e causar uma violação de segurança. As ameaças podem ser naturais (como desastres naturais), humanas (como ataques de hackers) ou causadas por erros não intencionais (como exclusão acidental de dados).

A pessoa ou coisa que representa uma ameaça é chamada de ator de ameaça ou agente de ameaça. O caminho ou ferramenta usada por um agente de ameaça mal-intencionado pode ser chamado de vetor de ataque.

Risco

O risco é a probabilidade de que uma ameaça explore uma vulnerabilidade específica e cause danos. Ele é frequentemente expresso como uma combinação da probabilidade de ocorrência de uma ameaça e do impacto potencial dos danos. Para avaliar riscos, devemos identificar uma vulnerabilidade e então avaliar a probabilidade de que ela venha a ser explorada por uma ameaça e, assim, calcular o impacto que a exploração bem-sucedida poderia trazer: $\text{risco} = \text{probabilidade} \times \text{impacto}$.



Risco e incerteza.

Estratégias para gerenciar riscos

É importante ressaltar que a Segurança da Informação busca reduzir o risco identificando vulnerabilidades, avaliando ameaças potenciais e implementando medidas de segurança adequadas para mitigar ou aceitar riscos a um nível considerado admissível. As estratégias adotadas na gestão de riscos são:

1. **Aceitação de risco:** em alguns casos, pode ser admissível aceitar certo nível de risco. Isso pode ocorrer quando os custos de mitigação superam os benefícios.
2. **Mitigação:** isso envolve a implementação de medidas de segurança para reduzir a probabilidade de uma ameaça explorar uma vulnerabilidade. Isso pode incluir patches de segurança, firewalls e treinamento de pessoal.
3. **Transferência de risco:** isso envolve a transferência de parte do risco para outra parte, como um seguro contra ciberataques.
4. **Evitação:** evitar um risco significa eliminar a vulnerabilidade ou a ameaça. Isso pode envolver, por exemplo, descontinuar o uso de um software obsoleto.

Matriz de risco

A matriz de risco em segurança da informação é uma ferramenta que ajuda as organizações a avaliar e visualizar os riscos de segurança relacionados às suas operações, sistemas, ativos de informação e processos. Ela é usada para classificar e priorizar os riscos com base em sua probabilidade de ocorrência e no impacto potencial que podem ter nas operações e na segurança da informação. É geralmente representada em forma de tabela, onde as ameaças, vulnerabilidades, riscos e medidas de mitigação são listados e classificados. Os elementos principais em uma matriz de risco incluem:

- **Ameaças:** são listadas as diversas ameaças ou eventos que podem afetar a segurança da informação. Exemplos incluem malware, ataques de hackers, desastres naturais, erro humano, entre outros.
- **Vulnerabilidades:** são identificadas as vulnerabilidades nos sistemas, processos ou ativos de informação que poderiam ser exploradas pelas ameaças. Isso pode incluir sistemas desatualizados, falta de controle de acesso ou deficiências na segurança física.
- **Riscos:** para cada combinação de ameaça e vulnerabilidade, é calculado o risco associado. Isso geralmente é feito atribuindo valores para a probabilidade de ocorrência da ameaça e o impacto potencial da exploração da vulnerabilidade.
- **Medidas de mitigação:** para cada risco, são identificadas as medidas de mitigação que podem ser implementadas para reduzir a probabilidade de ocorrência ou o impacto do risco. Isso pode incluir ações como atualizar software, treinar funcionários, implementar firewalls, entre outras.

A matriz de risco ajuda as organizações a priorizar os riscos com base em sua gravidade e probabilidade. Os riscos mais críticos e prováveis recebem maior atenção e recursos para a implementação de medidas de segurança. Ela também auxilia na comunicação dos riscos para partes interessadas, como a alta administração e equipes de segurança, e fornece um guia para o planejamento de estratégias de segurança da informação.

A criação e manutenção de uma matriz de risco é uma prática importante em segurança da informação, e está intimamente ligada à gestão de riscos. À medida que os ambientes digitais evoluem e as ameaças mudam, a matriz de risco deve ser atualizada regularmente para refletir as condições atuais e garantir que as estratégias de segurança estejam alinhadas com os riscos mais relevantes.

Impacto

Alto	Média	Alta	Alta
Médio	Baixa	Média	Alta
Baixo	Baixa	Baixa	Média
	Baixo	Médio	Alto

Probabilidade

Matriz de risco.


Principais tarefas de segurança cibernética com base no NIST Framework

NIST Cybersecurity Framework

O Framework de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST), conhecido como NIST Cybersecurity Framework, é uma abordagem amplamente reconhecida para ajudar as organizações a projetar, implementar e gerenciar estratégias de segurança cibernética eficazes. A estrutura básica fornece um conjunto de atividades para alcançar resultados específicos de segurança cibernética e faz referência a exemplos de diretrizes para que esses resultados sejam alcançados. O framework é composto por quatro elementos:

1. **Funções:** organizam atividades básicas de segurança cibernética em seu nível mais alto. Essas funções são: Identificar, Proteger, Detectar, Responder e Recuperar. Elas auxiliam uma organização a demonstrar seu gerenciamento de riscos de segurança cibernética, organizando as informações, possibilitando decisões de gerenciamento de riscos, tratando ameaças e aprimorando com base em atividades anteriores. As funções também se alinham com as metodologias existentes para o gerenciamento de incidentes e ajudam a mostrar o impacto dos investimentos em segurança cibernética. Por exemplo, os investimentos em planejamento e treinamento compreendem ações de resposta e recuperação em tempo hábil, resultando em um impacto reduzido na entrega de serviços.

2. **Categorias:** São as subdivisões de uma função em grupos de resultados de segurança cibernética, intimamente ligados a necessidades programáticas e atividades específicas. Exemplos de categorias incluem "Gerenciamento de ativos", "Gerenciamento de identidades e controle de acesso" e "Processos de detecção".
3. **Subcategorias:** desmembram uma categoria em resultados específicos de atividades técnicas e/ou de gerenciamento. Elas fornecem um conjunto de resultados que, embora não sejam exaustivos, ajudam a dar embasamento para a concretização dos resultados de cada categoria. Alguns exemplos de subcategorias: "Catalogação de sistemas de informação externos", "Proteção de dados em repouso" e "Investigação de notificações de sistemas de detecção".
4. **Referências informativas:** são seções específicas sobre normas, diretrizes e práticas comuns entre os setores de infraestrutura crítica que ilustram um método para alcançar os resultados relacionados a cada subcategoria. As referências informativas apresentadas na estrutura básica são ilustrativas e exemplificativas. Elas são baseadas em orientações intersetoriais referenciadas com maior frequência durante o processo de desenvolvimento da estrutura.

 National Institute of Standards and Technology		
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

Estrutura básica NIST.

Tarefas do NIST Framework

As cinco funções da estrutura básica são apresentadas abaixo. Essas funções não se destinam a formar um caminho sequencial ou levar a um estado final engessado. Em vez disso, as funções devem ser executadas simultaneamente e continuamente para criar uma cultura operacional que lide com o risco dinâmico da segurança cibernética.

1. **Identificar (Identify):** desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos. A partir da compreensão do contexto de seu nicho, dos recursos que suportam as funções críticas e dos riscos de segurança cibernética envolvidos, uma organização é capaz de focar e priorizar seus esforços de forma consistente com sua estratégia de gerenciamento de riscos e demandas empresariais. Os exemplos de categorias de resultados dentro desta função incluem:
 - **Gerenciamento de ativos:** os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos de negócio são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.
 - **Ambiente empresarial:** a missão, objetivos, stakeholders e atividades da organização são compreendidas e priorizadas. Essas informações serão usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.
 - **Governança:** as políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulatórios, jurídicos, de risco, ambientais e operacionais da organização são compreendidos e informam gerenciamento do risco de segurança cibernética.
 - **Avaliação de risco:** a organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos. São realizadas avaliações de vulnerabilidades para identificar fraquezas nos sistemas. Podem ser utilizadas ferramentas de varredura de vulnerabilidades e auditorias de segurança regulares. É importante manter-se atualizado sobre as ameaças atuais, como novos tipos de malware, táticas de hackers e vulnerabilidades emergentes. Participar de comunidades de segurança, consultar fontes confiáveis e avaliar relatórios de incidentes. Determinar o impacto potencial de ameaças em seus

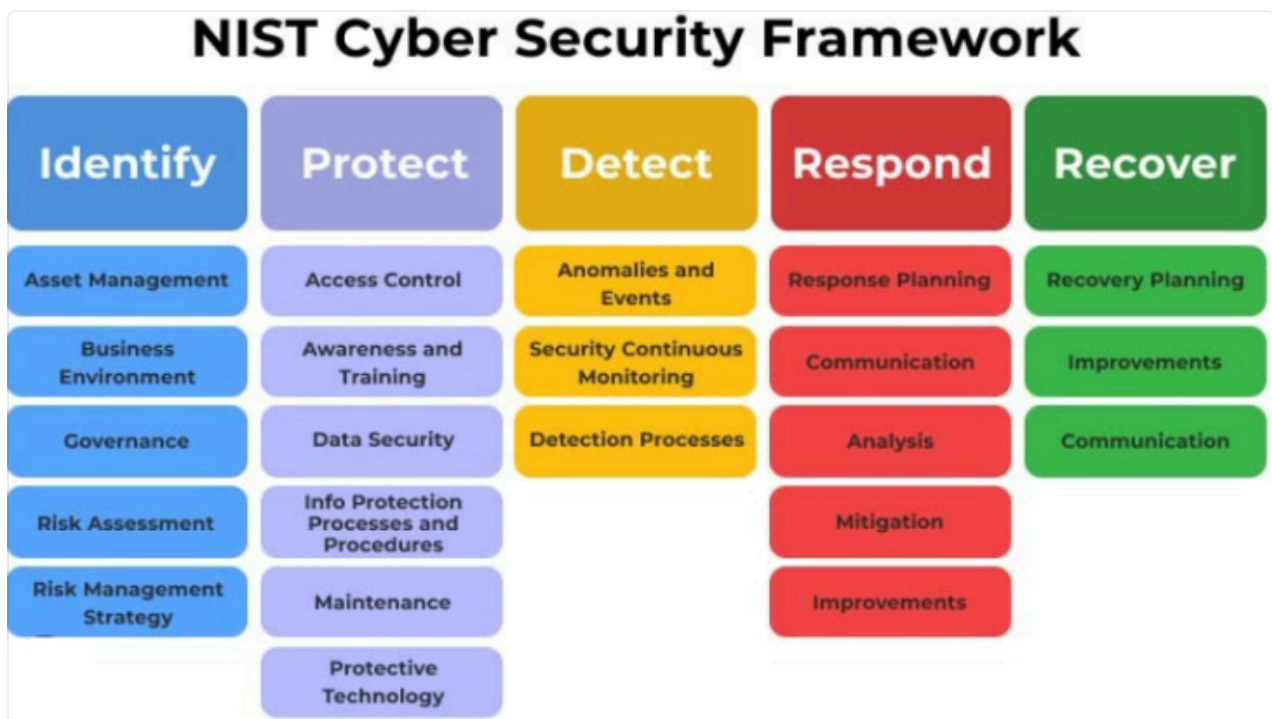
ativos críticos. Isso envolve a identificação de quais ativos são mais vitais para suas operações e a análise de como sua perda afetaria a organização. A partir daí, elaborar a classificação e as respostas aos riscos.

- **Estratégia de gerenciamento de risco:** as prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.
2. **Proteger (Protect):** desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos. A função *proteger* fornece apoio à capacidade de limitar ou conter o impacto de uma possível ocorrência de segurança cibernética. Os exemplos de categorias de resultados dentro dessa função incluem:
- **Controle de acesso:** o acesso a ativos físicos e lógicos e recursos associados é limitado a usuários, processos e dispositivos autorizados, e é gerenciado de maneira consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas. Implemente políticas de controle de acesso, como a autenticação de dois fatores, gerenciamento de senhas fortes e controles de acesso baseados em função. Isso restringirá o acesso apenas a pessoas autorizadas.
 - **Gerenciamento de identidade:** utilize sistemas de gerenciamento de identidade para criar, manter e revogar credenciais de acesso. Isso garantirá que apenas pessoas autorizadas tenham acesso aos recursos.
 - **Conscientização e treinamento:** os funcionários e parceiros da organização são treinados sobre a conscientização sobre segurança cibernética e são treinados para executar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com os procedimentos e acordos relacionados. Realizar treinamentos regulares de conscientização em segurança cibernética para educar os funcionários sobre as ameaças e boas práticas ajudará a reduzir o risco de ataques de engenharia social.
 - **Segurança de dados:** as informações e os registros (dados) são gerenciados de maneira consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade de informações.
 - **Processos e procedimentos de proteção da informação:** as políticas de segurança (que abordam a finalidade, o escopo, as funções, as responsabilidades, o compromisso de gerenciamento e a coordenação entre as entidades organizacionais), processos e procedimentos são mantidas e usadas para gerenciar a proteção de sistemas e ativos de informações.

- **Manutenção:** a manutenção e os reparos de componentes de sistemas de controle e informações industriais são executados de acordo com políticas e procedimentos. Mantenha sistemas e aplicativos adequadamente configurados e atualizados. Utilize políticas de configuração e automação de gerenciamento de configuração para manter a consistência.
 - **Tecnologia de proteção:** as soluções de segurança técnica são gerenciadas para garantir a segurança e resiliência de sistemas e ativos, consistentes com políticas, procedimentos e acordos relacionados.
3. **Detectar (Detect):** desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética. A função *detectar* permite a descoberta oportuna de ocorrências de segurança cibernética. Os exemplos de categorias de resultados dentro dessa função incluem:
- **Anomalias e ocorrências:** atividade anômala é detectada e o impacto potencial dos eventos é compreendido.
 - **Monitoramento contínuo de segurança:** o sistema de informação e os ativos são monitorados para identificar incidentes de segurança cibernética e verificar a eficácia das medidas de proteção. Implementar ferramentas de monitoramento de segurança que alertem sobre atividades suspeitas em tempo real. Isso pode incluir sistemas de detecção de intrusões, registros de eventos e monitoramento de rede.
 - **Processos de Detecção:** os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização sobre eventos anômalos. Significa desenvolver processos para analisar eventos de segurança em tempo real e determinar se são incidentes reais. Criar regras e procedimentos para identificar atividades anômalas.
4. **Responder (Respond):** desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado. A função *responder* suporta a capacidade de conter o impacto de um possível incidente de segurança cibernética. Exemplos de categorias de resultados dentro dessa função incluem:
- **Planejamento de resposta:** os processos e procedimentos de resposta são executados e mantidos para garantir a resposta a incidentes de segurança cibernética detectados. Desenvolva planos de resposta a incidentes que

definam funções e responsabilidades, procedimentos de notificação, comunicação com partes interessadas e ações para conter o incidente.

- **Comunicações:** as atividades de resposta são coordenadas com stakeholders internos e externos (por exemplo, apoio externo de órgãos fiscalizadores). Crie um protocolo de comunicação para notificar as partes interessadas sobre um incidente de segurança. Isso pode incluir reguladores, clientes e a equipe de resposta a incidentes.
 - **Análise:** a análise é realizada para garantir resposta eficaz e dar apoio às atividades de recuperação.
 - **Mitigação:** as atividades são realizadas para impedir a expansão de um evento, atenuar seus efeitos e resolver o incidente.
 - **Aperfeiçoamentos:** as atividades de resposta organizacionais são aperfeiçoadas pela incorporação de lições aprendidas de atividades anteriores de detecção/resposta.
5. **Recuperar (Recover):** desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética. A função *recuperar* oferece apoio ao restabelecimento pontual para as operações normais de modo a reduzir o impacto de determinado incidente de segurança cibernética. Os exemplos de categorias de resultados dentro dessa função incluem:
- **Planejamento de recuperação:** os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração de sistemas ou ativos afetados por incidentes de segurança cibernética. Desenvolva planos de continuidade de negócios que garantam que a organização possa continuar a operar após um incidente. Isso pode envolver o uso de data centers de recuperação de desastres, locais alternativos de trabalho etc.
 - **Aperfeiçoamentos:** o planejamento e os processos de recuperação são aperfeiçoados pela incorporação de lições aprendidas em atividades futuras.
 - **Comunicações:** as atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, provedores de serviços de Internet, proprietários de sistemas de ataque, vítimas, outras CSIRTs e fornecedores).



NIST Framework.

Conclusão

Parabéns por ter finalizado a aula sobre Princípios de Segurança da Informação! Nesta aula, exploramos os princípios fundamentais da Segurança da Informação, incluindo a tríade CID (Confidencialidade, Integridade e Disponibilidade), a relação entre vulnerabilidade, ameaça e risco, e as principais tarefas de segurança cibernética com base no Framework de Segurança Cibernética do NIST.

A tríade CID serve como alicerce, lembrando-nos constantemente da importância de manter a confidencialidade dos dados, garantir sua integridade contra modificações não autorizadas e assegurar que eles estejam disponíveis quando necessários.

Além disso, a relação entre vulnerabilidade, ameaça e risco nos mostra como as ameaças exploram as vulnerabilidades para criar riscos que podem impactar negativamente as operações e a segurança da informação. A identificação, avaliação e mitigação desses riscos são tarefas críticas na segurança da informação.

Por fim, o Framework de Segurança Cibernética do NIST fornece uma estrutura sólida para que as organizações planejem e implementem estratégias eficazes de segurança cibernética. Ao seguir as fases de Identificar, Proteger, Detectar, Responder e Recuperar, as organizações podem fortalecer sua postura de segurança, mitigar ameaças e responder aos incidentes de forma eficaz.

Aula 2: Profissionais em Segurança da Informação

Objetivos

- ☒ Compreensão dos papéis e responsabilidades.
- ☒ Conhecimento das unidades de negócios de segurança.
- ☒ Familiaridade com metodologias ágeis.

Conceitos

- ☒ Papéis e responsabilidades dos profissionais de segurança da informação.
- ☒ Unidades de negócio NOC e SOC.
- ☒ Metodologias de trabalho ágeis como Kanban, XP, Scrum, DevOps e DevSecOps.

Introdução

Bem-vindos à aula 1.2 do nosso curso de Segurança da Informação. Na aula anterior, abordamos os fundamentos da Segurança da Informação, destacando a sua importância em um mundo cada vez mais digital e interconectado. Hoje, daremos um passo adiante, estudando como os diferentes profissionais operam nesse campo dinâmico e vital.

A Segurança da Informação não é apenas uma questão técnica, mas é também uma disciplina que envolve pessoas, processos e tecnologia. Nesta aula, vamos abordar os diversos papéis e responsabilidades que os profissionais em Segurança da Informação desempenham em organizações de todos os tamanhos. Desde os estrategistas, que moldam a visão de segurança, até os especialistas, que identificam e mitigam ameaças, todos têm um papel fundamental a desempenhar.

Além disso, exploraremos as unidades de negócios de Segurança da Informação, conhecidas como NOC, SOC e CSIRT, e os times especializados, como Blue Team, Red Team, Purple Team e White Team. Compreender como essas unidades trabalham juntas é crucial para uma defesa eficaz contra ameaças cibernéticas.

Por fim, abordaremos a integração de metodologias de trabalho ágil no contexto da Segurança da Informação. Veremos como práticas como Kanban, XP, Scrum, DevOps e DevSecOps podem acelerar a resposta a incidentes e fortalecer a postura de segurança de uma organização.

Competências de Segurança da Informação

A Segurança da Informação passa pelo entendimento da diversidade de profissionais que desempenham papéis fundamentais na proteção das informações e ativos digitais. Os profissionais de TI que trabalham em funções com responsabilidades de segurança devem ser competentes em uma ampla gama de disciplinas, desde projeto de redes e aplicações até compras e recursos humanos. As seguintes atividades podem ser típicas de cada função:

- Participar de avaliações de risco e testes de sistemas de segurança e fazer recomendações.
- Especificar, prover, instalar e configurar dispositivos e softwares de segurança.
- Configurar e manter controle de acesso a documentos e perfis de privilégio de usuário.
- Monitorar registros de auditoria, revisar privilégios de usuários e controlar o acesso a documentos.
- Gerenciar resposta a incidentes e relatórios relacionados à segurança.
-

Criar e testar os Planos de Continuidade de Negócio e de Recuperação de Desastres e Procedimentos.

- Participar de programas de treinamento e educação em segurança.



Competências em cibersegurança.

Papéis e responsabilidades em Segurança da Informação

A seguir, veremos os papéis dos profissionais em Segurança da Informação, desde o estrategista-chefe, que define as políticas de segurança; até o especialista, que identifica vulnerabilidades; e o cientista de dados, que analisa ameaças. Vamos entender como elas se encaixam no desenho da cibersegurança. Os principais profissionais no campo de Segurança da Informação, destacando seus papéis e responsabilidades, são:

1. **CISO (Chief Information Security Officer):** a responsabilidade interna geral pela segurança pode ser executada por um departamento dedicado, administrado

por um Diretor de Segurança (CSO) ou um Diretor de Segurança da Informação (CISO). Embora, historicamente, a responsabilidade pela segurança tem sido atribuída a uma unidade de negócios existente, como Tecnologia da Informação e Comunicação (TIC).

Papel: o CISO é o líder sênior de Segurança da Informação. Ele é o principal responsável pela Segurança da Informação em uma organização. Seu papel de liderança é fundamental na definição de estratégias de segurança, na gestão de riscos cibernéticos e na supervisão das equipes de segurança.

Responsabilidades:

- Desenvolver e implementar políticas de Segurança da Informação.
- Supervisionar equipes de segurança.
- Garantir conformidade com regulamentações de segurança.
- Avaliar e mitigar riscos de segurança.
- Responder aos incidentes de segurança.

2. **DPO (Data Protection Officer):** o DPO, ou Data Protection Officer, é um profissional cuja função central é garantir que uma organização esteja em conformidade com regulamentações de privacidade de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, e a Lei Geral de Proteção de Dados (LGPD), no Brasil. O DPO desempenha um papel crítico na proteção dos dados pessoais dos indivíduos e no fortalecimento da privacidade em uma organização. Ele auxilia na proteção dos dados pessoais dos clientes.

Papel: o DPO tem o papel de fazer a ponte entre a organização e a autoridade nacional de proteção de dados, garantindo que a organização cumpra regulamentações de privacidade de dados.

Responsabilidades:

- Monitorar e aconselhar sobre o tratamento de dados pessoais.
 - Elaborar avaliação de Impacto de Proteção de Dados.
 - Garantir a conformidade com regulamentações de privacidade.
 - Revisar contratos e parcerias.
-

- Atuar como ponto de contato para autoridades de proteção de dados.
 - Responder pela comunicação com os titulares dos dados.
 - Educar os funcionários sobre políticas de privacidade.
3. **Analista de Segurança da Informação:** esse profissional atua no gerenciamento da infraestrutura de TI. Ele também desempenha um papel fundamental na implementação de medidas de segurança.

Papel: seu papel é técnico-analítico, desempenhando funções no monitoramento da infraestrutura de TI, identificando vulnerabilidades e respondendo aos incidentes de segurança.

Responsabilidades:

- Monitorar sistemas e redes em busca de atividades suspeitas.
 - Implementar medidas de segurança, como firewalls e antivírus.
 - Investigar e responder sobre incidentes de segurança.
 - Avaliar a eficácia das políticas de segurança.
4. **Hacker ético:** os hackers éticos (também conhecidos como pentesters) são contratados para testar a segurança de sistemas e aplicativos de uma organização.

Papel: o papel dos hackers éticos é atuar como um ator de ataque com consentimento para testar a segurança de sistemas e aplicativos, procurando vulnerabilidades e evitar que criminosos o façam.

Responsabilidades:

- Realizar testes de penetração em sistemas.
 - Identificar e relatar vulnerabilidades.
 - Simular ataques para avaliar a resistência das defesas.
 - Ajudar na melhoria da segurança da organização.
5. **Especialista em segurança em nuvem:** esses profissionais se concentram em disponibilizar recursos em nuvem com segurança e em conformidade com

padrões estabelecidos.

Papel: esses profissionais se concentram em garantir que os recursos na nuvem estejam seguros e em conformidade com as melhores práticas. Possui especialização em computação em nuvem.

Responsabilidades:

- Avaliar e configurar a segurança em ambientes de nuvem.
- Monitorar ameaças na nuvem.
- Implementar políticas de segurança na nuvem.
- Garantir a conformidade com regulamentações em nuvem.

6. **Analista de forense digital:** responsável pela investigação de incidentes de segurança, coleta de evidências eletrônicas em apoio a processos legais.

Papel: seu principal papel é atuar em investigações forenses, fornecendo suporte a processos legais.

Responsabilidades:

- Coletar e analisar evidências digitais.
- Reconstruir incidentes de segurança.
- Preparar relatórios de forense digital para fins legais.
- Ajudar na identificação de invasores.

7. **Cientista de dados em segurança:** esses profissionais aplicam técnicas de análise de dados para identificar ameaças e tendências de segurança.

Papel: seu principal papel é analisar dados identificando comportamentos que possam ameaçar a segurança.

Responsabilidades:

- Analisar grandes conjuntos de dados para identificar padrões de ameaças.
-
- Desenvolver modelos preditivos de segurança.
-
- Monitorar o tráfego de rede em busca de atividades suspeitas.
-

- Identificar anomalias e ameaças em tempo real.
8. **Analista de resposta a incidentes de segurança:** encarregados de responder a incidentes de segurança, mitigar danos e implementar medidas corretivas.

Papel: seu principal papel é atuar na linha de frente na ocorrência de incidentes de segurança.

Responsabilidades:

- Detectar e analisar incidentes de segurança.
 - Isolar e conter ameaças.
 - Recuperar sistemas após um incidente.
 - Documentar e reportar incidentes às partes interessadas.
9. **Testador de software:** testadores especializados em segurança que avaliam aplicativos em busca de vulnerabilidades.

Papel: seu principal papel é atuar no aperfeiçoamento da segurança dos aplicativos, buscando vulnerabilidades que devem ser corrigidas.

Responsabilidades:

- Realizar testes de segurança em aplicativos e sistemas.
- Identificar vulnerabilidades, como falhas de injeção SQL ou cross-site scripting.
- Trabalhar com equipes de desenvolvimento para corrigir falhas de segurança.
- Validar a eficácia das correções implementadas.



CISO.

Unidades de negócios de Segurança da Informação

As unidades, conforme descritas abaixo, desempenham um papel na proteção da informação e dos ativos digitais de uma organização. A escolha de qual unidade implantar depende das necessidades específicas da organização, seu ambiente de ameaças e recursos disponíveis. A integração de várias dessas unidades pode fornecer uma abordagem holística mais efetiva para a segurança cibernética.

NOC (Network Operations Center)

O NOC — ou Network Operations Center — é uma unidade de negócios de Segurança da Informação que se concentra na monitorização, gestão e manutenção contínua da infraestrutura de rede da organização.

- **Objetivos:** monitorar a disponibilidade e o desempenho da rede, identificar e responder a problemas de rede em tempo real e garantir a continuidade das operações de rede.
-

Serviços executados: monitorização da rede 24/7, detecção de falhas na rede, respostas a incidentes de rede e manutenção de hardware de rede.

- **Vantagens:** garante disponibilidade e confiabilidade da rede, identifica e soluciona problemas de rede rapidamente e reduz o tempo de inatividade da rede.
- **Desvantagens:** foco limitado à infraestrutura de rede, excluindo segurança cibernética, e pode não abranger ameaças cibernéticas avançadas.



NOC.

SOC (Security Operations Center)

O SOC, ou Security Operations Center, é uma unidade de negócios de Segurança da Informação que monitora, detecta, responde e previne ameaças de segurança cibernética.

- **Objetivos:** monitorar e responder aos incidentes de segurança cibernética, identificar ameaças em tempo real e prevenir ataques cibernéticos.
- **Serviços executados:** monitorização de eventos de segurança, resposta a incidentes de segurança, análise forense digital e implementação de políticas de

segurança.

- **Vantagens:** protege contra ameaças cibernéticas, responde rapidamente aos incidentes de segurança e oferece visibilidade completa sobre a postura de segurança da organização.
- **Desvantagens:** requer recursos significativos para operação eficaz e pode gerar alertas em grande volume, resultando em falsos positivos.



SOC.

CSIRT (Computer Security Incident Response Team)

O CSIRT — ou Computer Security Incident Response Team — é uma unidade de negócios que se concentra na resposta a incidente de segurança cibernética. Pode ser parte do SOC ou uma equipe independente.

- **Objetivos:** responder eficazmente aos incidentes de segurança cibernética, isolar, mitigar e corrigir vulnerabilidades e ameaças, e identificar a causa raiz de incidentes de segurança.
- **Serviços executados:** investigação de incidentes de segurança cibernética, mitigação de ameaças, análise forense digital e recuperação de sistemas afetados.
- **Vantagens:** expertise em resposta a incidentes de segurança, minimiza danos causados por incidentes e contribui para a aprendizagem contínua e melhoria da

segurança.

- **Desvantagens:** geralmente, atua após a ocorrência do incidente, e requer pessoal altamente treinado, além de recursos técnicos.



CSIRT.

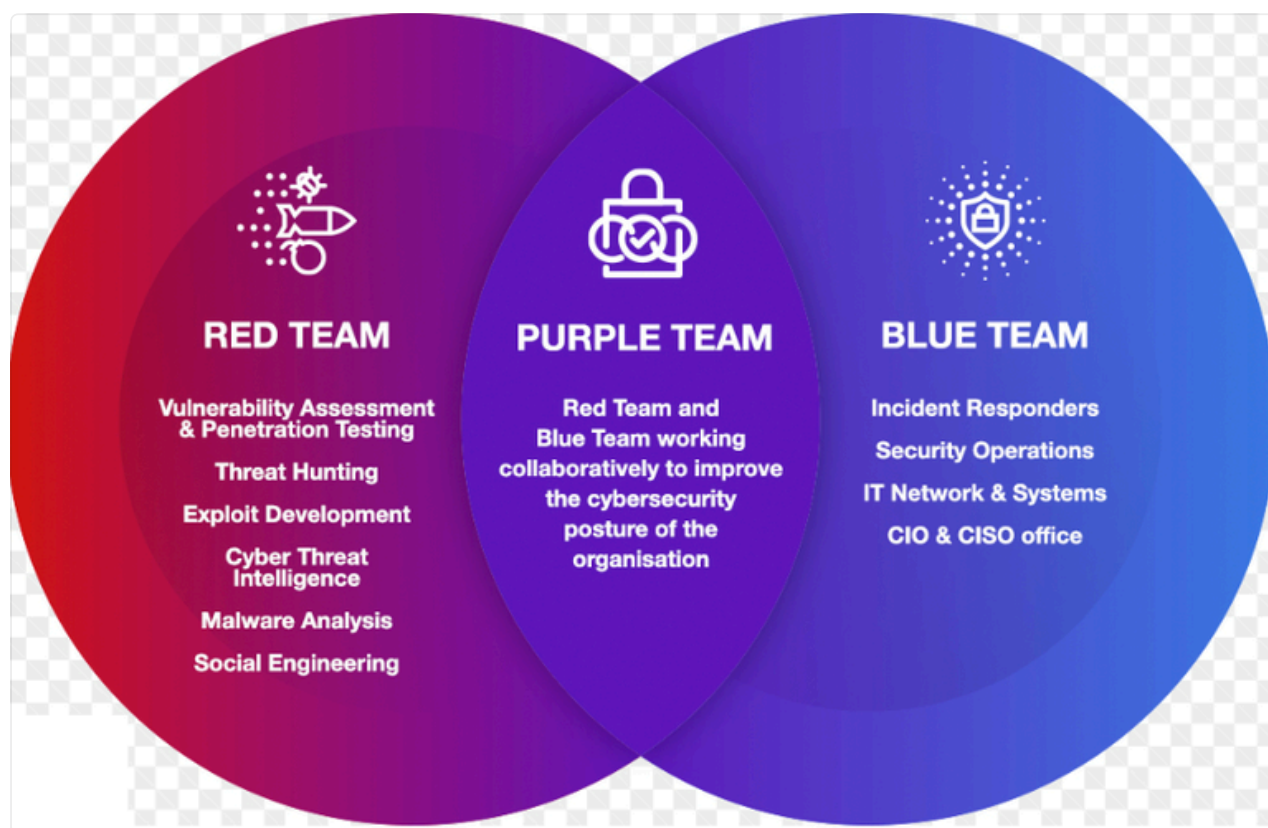
- **Times de teste (Blue Team, Red Team, Purple Team e White Team):** esses times são parte do SOC e CSIRT, e desempenham papéis específicos em testes de segurança e avaliações de postura de segurança:
- **Blue Team:** monitorização e defesa. Defesa e proteção contra ameaças cibernéticas. Equipe defensiva focada na proteção e detecção de ameaças.
- **Red Team:** simulação de ataques. Simulação de ataques para avaliar as defesas da organização. Equipe ofensiva que simula ataques para avaliar a eficácia das defesas.
- **Purple Team:** avaliação e aprimoramento de segurança. Colaboração entre Blue e Red Teams para avaliar e melhorar a segurança.
- **White Team:** validação de resultados de testes. Avalia e valida os resultados de testes de segurança, e garante a melhoria contínua.

Vantagens:

- Avaliação contínua da segurança.
- Identificação de vulnerabilidades antes de invasores reais.
- Melhoria da postura de segurança.

Desvantagens:

- Red Teams podem causar interrupções e exigir comunicação clara para evitar mal-entendidos.
- Requer recursos e planejamento adequado para ser eficaz.



Equipes de segurança.

Metodologias de trabalho ágil

Cada metodologia ágil tem seu próprio conjunto de princípios e práticas que atendem a diferentes necessidades e contextos. A escolha da metodologia a ser adotada depende das características do projeto, da cultura organizacional e dos objetivos específicos a serem alcançados. A integração de DevOps e DevSecOps enfatiza a importância de incorporar segurança e eficiência em todas as etapas do ciclo de desenvolvimento de software. A seguir, descrevemos as características de cada metodologia:

1. **Kanban:** é uma metodologia de gerenciamento visual que se concentra em controlar o fluxo de trabalho. Ela é baseada em placas ou quadros Kanban, que

representam tarefas em diferentes estágios de conclusão. A abordagem visual de gerenciamento de tarefas auxilia as equipes no acompanhamento e priorização do trabalho.

- **Objetivos:** controlar o fluxo de trabalho de forma eficiente, identificar gargalos e atrasos nas tarefas e maximizar a produtividade.
- **Principais funções:** visualização do fluxo de trabalho, limites de trabalho em progresso (WIP – Work in Progress) e priorização contínua de tarefas.
- **Vantagens:** flexibilidade para lidar com tarefas de diferentes complexidades, foco na entrega contínua de valor e identificação rápida de problemas no processo de trabalho.
- **Desvantagens:** pode ser menos prescritiva, o que exige maior autodisciplina da equipe, requer monitorização constante para evitar acumulação de trabalho.

2. **XP (Extreme Programming):** é uma metodologia de desenvolvimento de software ágil que enfatiza a colaboração, feedback contínuo e entrega de software de alta qualidade. Ela se baseia em práticas como desenvolvimento orientado a testes (TDD) e programação em pares.

- **Objetivos:** melhorar a qualidade do software, entregar valor ao cliente rapidamente e manter a flexibilidade e adaptabilidade.
- **Principais Funções:** programação em pares, testes automatizados e integração contínua.
- **Vantagens:** software mais robusto e confiável, entregas frequentes e incrementais e foco na satisfação do cliente.
- **Desvantagens:** requer treinamento e adoção cultural, pode ser menos eficaz em projetos muito grandes.

3. **Scrum:** é um framework de desenvolvimento ágil iterativo que divide o projeto em ciclos curtos chamados "sprints", com duração fixa. Ele foca em entregas frequentes, enfatiza a colaboração, comunicação e adaptação contínua.

- **Objetivos:** entrega de software iterativa, adaptação rápida a mudanças de requisitos, e comunicação e colaboração eficazes.
- **Principais funções:**
Scrum Master: facilita o processo Scrum; Product Owner: define e prioriza requisitos; time de desenvolvimento: implementa funcionalidades.

-

Vantagens: entregas regulares de funcionalidades, foco na transparência e adaptação, comunicação clara.

- **Desvantagens:** pode ser menos eficaz em projetos muito pequenos ou muito grandes, e requer comprometimento e papel claro de todos os membros da equipe.
4. **DevOps:** é uma cultura e conjunto de práticas que integra o desenvolvimento de software e operações. Acelera a entrega de software de alta qualidade e reduz barreiras entre equipes.
- **Objetivos:** entrega rápida e confiável de software, automação de processos e colaboração entre desenvolvimento e operações.
 - **Principais funções:** desenvolvedores, Operações de TI e engenheiros de automação.
 - **Vantagens:** entregas frequentes e confiáveis, redução de falhas de implantação e colaboração e eficiência.
 - **Desvantagens:** implementação e adoção cultural desafiadoras, requer investimento em automação.
5. **DevSecOps:** é uma extensão do DevOps que inclui a segurança como parte integrante do ciclo de desenvolvimento e implantação de software. A integração da segurança nas práticas DevOps serve para garantir que a segurança seja uma parte intrínseca do ciclo de vida do desenvolvimento.
- **Objetivos:** integração de segurança em todo o ciclo de vida do software, identificação precoce de vulnerabilidades e proteção contra ameaças cibernéticas.
 - **Principais funções:** segurança da Informação, engenheiros de segurança e desenvolvedores.
 - **Vantagens:** maior segurança do software, identificação precoce de ameaças cibernéticas e conformidade regulatória.
 - **Desvantagens:** necessita de treinamento e conscientização sobre segurança em toda a equipe, e pode adicionar complexidade ao processo de desenvolvimento.



Metodologia Ágil.

Conclusão

Chegamos ao fim da nossa aula sobre profissionais em cybersecurity. Estudamos aqui os setores dentro das organizações, denominados unidades de negócios, onde as funções de segurança da informação são executadas. Vimos, também, as metodologias ágeis mais utilizadas, e esperamos que vocês tenham adquirido um entendimento sólido sobre os diversos papéis e responsabilidades desempenhadas por profissionais da área. Ressaltamos a importância das unidades de negócios dedicadas a proteger ativos digitais e a eficácia das metodologias ágeis na cibersegurança.

Lidar com as ameaças cibernéticas e proteger as informações da organização são responsabilidades de todos. Cada um dos profissionais abordados tem um papel crucial nessa missão, contribuindo para um ambiente digital mais seguro.

Parabéns a todos pela conclusão desta aula! Vocês deram um passo importante no caminho para se tornarem profissionais qualificados em Segurança da Informação. Estamos ansiosos para compartilhar mais conhecimento e desafios com vocês na próxima aula. Até lá!