IDESP
Instituto Daryus
de Ensino Superior
Paulista

NIST
CYBERSECURITY FRAMEWORK

Check-In

NOME E EMPRESA

EXPERIÊNCIA PROFISSIONAL

OBJETIVO - EXPECTATIVA

CONTEÚDO

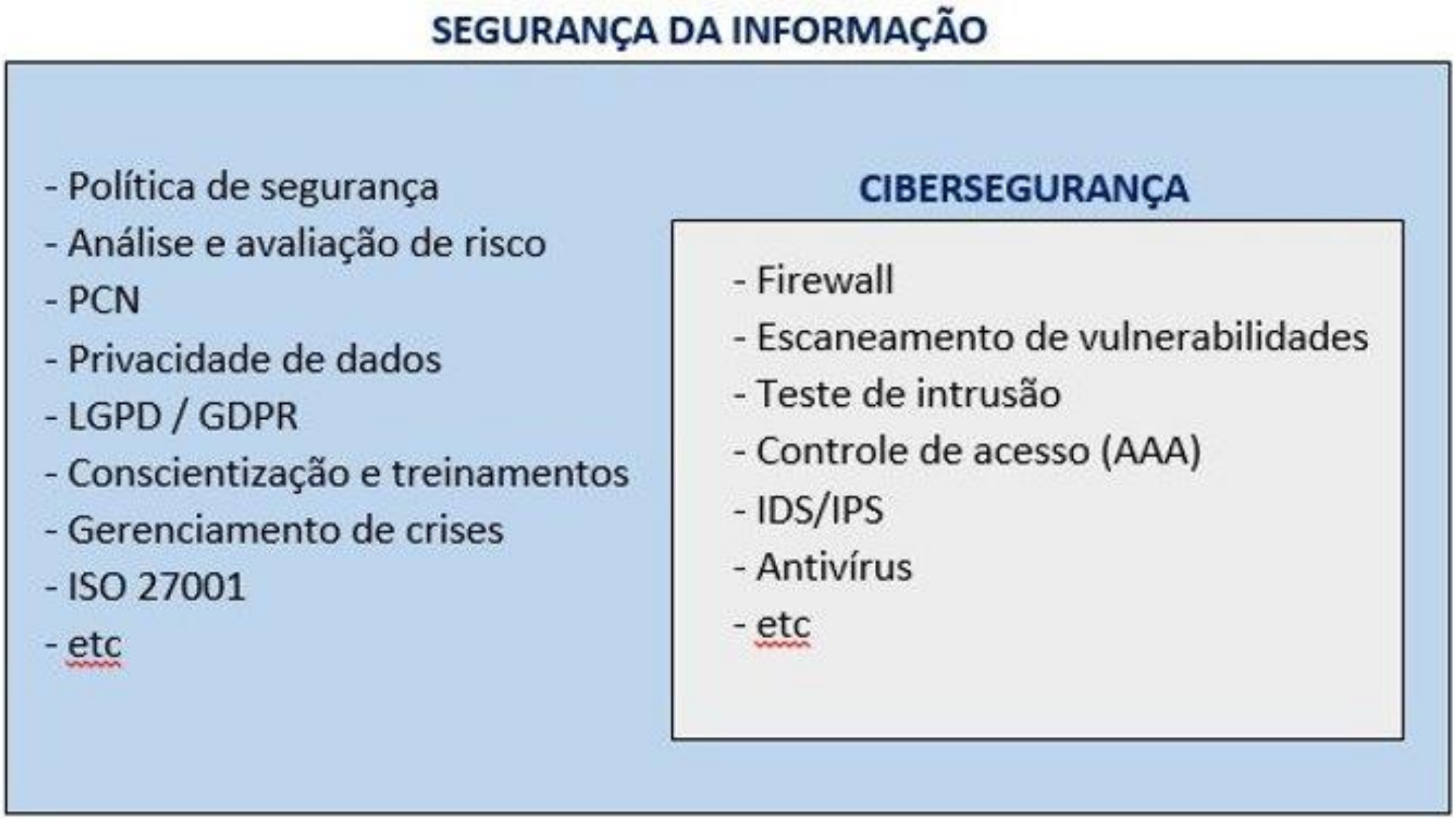
NIST - CSF

- Módulo 1: Introdução
- Módulo 2: O NIST Cyber Security Framework (CSF)
- Módulo 3: Governar
- Módulo 4: Identificar
- Módulo 5: Proteger
- Módulo 6: Detectar
- Módulo 7: Responder
- Módulo 8: Recuperar
- Avaliação

INTRODUÇÃO

- Confidencialidade
- Disponibilidade
- Integridade
- Responsabilização (não-repúdio) - O princípio da irretratabilidade
- Autenticação
- Autorização

Introdução Segurança da informação vs cibersegurança



Introdução

- Confidencialidade
- Disponibilidade
- Integridade
- Responsabilização (não-repúdio) - O princípio da irretratabilidade
- Autenticação
- Autorização

Hash e Criptografia

IDESP
Instituto Daryus
de Ensino Superior
Paulista

- **Hash** - MD5, SHA-1, SHA-256, PBKDF2, bcrypt, scrypt, Argo2
  - São funções de hash de mão única e não podem ser revertidos.
  - Utilizados para integridade de textos e arquivos e no armazenamento de senhas em bancos de dados

- **Criptografia**
  - Na criptografia propriamente dita, os dados podem ser revertidos mas necessitam da chave criptográfica.
  - Chaves podem ser simétricas ou assimétricas
  - Garante a confidencialidade das informações

Hash e Criptografia

IDESP
Instituto Daryus
de Ensino Superior
Paulista

- Criptografía **simétrica** - DES, 3DES, RC5, AES, Blowfish
  - Utiliza a mesma chave tanto para criptografar quanto para descriptografar os dados

- Criptografia **assimétrica** – Diffie-Helman, RSA, ElGamal
  - Utiliza um par de chaves, uma para criptografar e outra para descriptografar

daryus

NIST
CYBERSECURITY FRAMEWORK

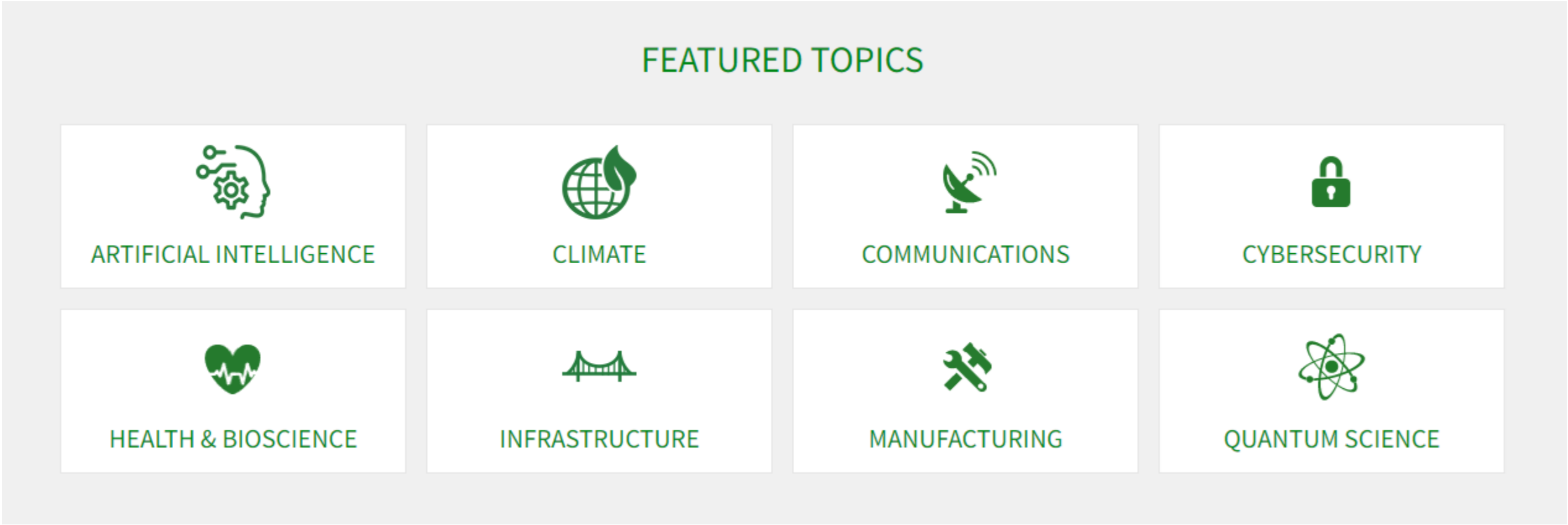
Módulo 2:
O NIST Cyber Security Framework

CREDENCIADO
HSI INSTITUTE

O NIST

- **NIST:** *National Institute of Standards and Technology*
  - Instituto Nacional de Padrões e Tecnologia
- Sua missão é promover a inovação e competitividade industrial dos Estados Unidos.
- Promove a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.
- Na década desde que foi publicado pela primeira vez, o CSF foi baixado mais de dois milhões de vezes por utilizadores em mais de 185 países e foi traduzido para pelo menos nove idiomas.

- Principais pesquisas suportadas pelo NIST:



- Categorias de publicações:
  - **FIPS:** *Federal Information Processing Standards*
    - Padrões de segurança.
  - **SP:** NIST *Special Publications*
    - Especificações técnicas, guias e melhores práticas.
  - **NISTIR:** NIST *Internal or Interagency Reports*
    - Relatórios de pesquisa, incluindo a fundamentação teórica para os FIPS e SPs.
  - **ITL Bulletin:** NIST *Information Technology Laboratory* (ITL) *Bulletins*
    - *Overviews* mensais das publicações e projetos do NIST.

- Algumas **SP**s:
  - SP 800: *Computer Security*
  - SP 1800: *Cybersecurity practice guides*
  - SP 500: *Information technology* (documentos relevantes)

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

- https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

FISMA

- Federal Information Security Modernization Act

Documentos FISMA do ano fiscal de 2023

Métricas do CIO FISMA para o ano fiscal de 2023

Baixar arquivo (PDF, 581,66 KB)

Métricas IG FISMA AF23-24

PUBLICAÇÃO

Baixar arquivo (PDF, 761,36 KB)

Guia de avaliação de métricas IG FISMA para o ano fiscal de 2023

PUBLICAÇÃO

Baixar arquivo (PDF, 1,19 MB)

- https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

NICE

IDESP
Instituto Daryus de Ensino Superior Paulista

Unveiling NICE Framework Components v1.0.0: Explore the Latest Updates Today!

March 05, 2024

NICE Framework Components v1.0.0

Credit: NICE Program Office

NICE Framework components version 1.0.0 comprises Work Role Categories, Work Roles, Competency Areas, and Task, Knowledge, and Skill (TKS) statements as well as the relationships between those elements. Previously released in 2017 as the Reference Spreadsheet, the NICE Framework components have had a full refresh and update of content based on feedback from recent calls for comment.

ORGANIZATIONS

Information Technology Laboratory
Applied Cybersecurity Division
NICE

SIGN UP FOR UPDATES FROM NIST

Enter Email Address

Sign up

- https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started

Executando o Framework

Aplicando o Framework

https://www.nist.gov/cyberframework

Executando o Framework

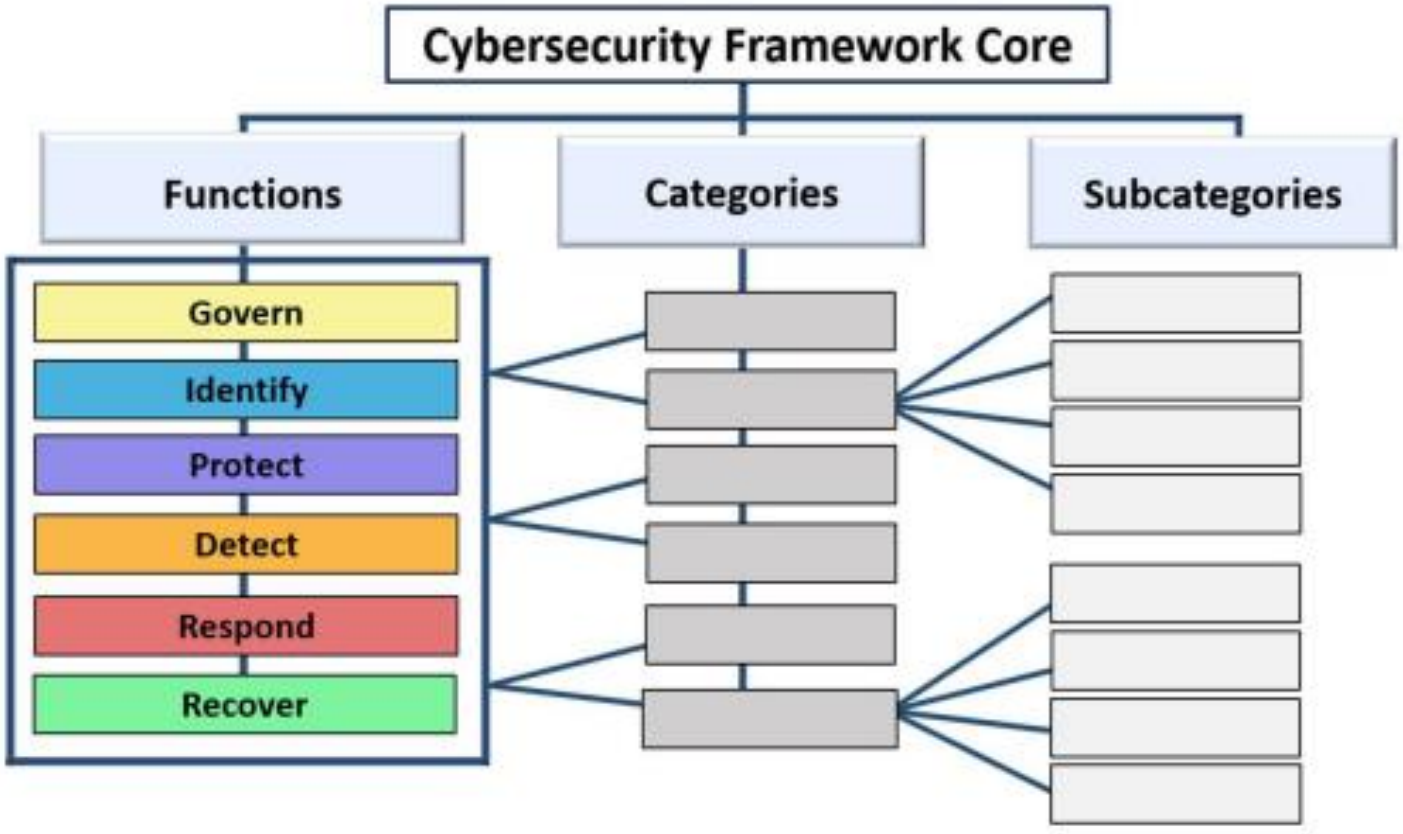


Fig. 1. CSF Core structure

Aplicando o Framework

https://www.nist.gov/cyberframework

O NIST CSF: Histórico

O NIST CSF: Histórico

- Fevereiro de 2013: *Executive Order* 13636.
  - Assinada por Barack Obama em 12 de fevereiro de 2013.
  - Estabelece diferentes requisitos para o desenvolvimento de um *framework* de cibersegurança para auxiliar as nações a protegerem suas infraestruturas críticas.
- Julho de 2013: A versão preliminar do *framework* é liberada ao público.

O NIST CSF: Histórico

- Fevereiro de 2014: A versão 1.0 do *framework* é disponibilizada oficialmente.
- Dezembro de 2014: *Cyber security enhancement act*.
- Abril de 2018: Versão 1.1 disponibilizada.
  - O *framework* evoluiu para ser mais informativo, útil e inclusivo para todos os tipos de organizações.
  - A versão 1.1 é totalmente compatível com a versão 1.0.
- Agosto de 2023: Rascunho da Versão 2.0 disponibilizada.
- 2024 Atualização definitiva.

O NIST CSF: Benefícios

- O CSF fornece uma linguagem comum e metodologia sistemática para gerenciar riscos de cibersegurança.

- Organizações podem identificar áreas nas quais os processos existentes precisam ser fortalecidos ou onde novos processos podem ser implementados.

Categorias

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

O NIST CSF: Camadas

IDESP
Instituto Daryus
de Ensino Superior
Paulista

- Existem **quatro camadas** (ou *tiers*) de implementação descritas pelo NIST.

- Quanto maior a camada, mais próximo o programa de gerenciamento de riscos de segurança cibernética da organização está das características definidas na estrutura.

O NIST CSF: Camadas

- Os níveis descrevem um grau crescente de rigor e sofisticação nas práticas de gerenciamento de riscos de segurança cibernética.

- Os níveis ajudam a determinar até que ponto o gerenciamento do risco de segurança cibernética é eficaz na sua organização.

O NIST CSF: Camadas

- As quatro camadas são:
  - Nível 1: Parcial
  - Nível 2: Risco informado
  - Nível 3: Repetível
  - Nível 4: Adaptável

O NIST CSF: Camadas – Parcial

- As práticas de gerenciamento de risco de segurança cibernética organizacional não são formalizadas.
- Muitas vezes o risco é gerenciado de maneira reativa.
- Existe uma consciência limitada do risco de segurança cibernética no nível organizacional.
- A organização geralmente não tem consciência dos riscos da cadeia de suprimentos cibernéticos dos produtos e serviços que fornece e usa.

O NIST CSF: Camadas – Risco informado

- As práticas de gerenciamento de risco são aprovadas pela administração, mas podem não ser estabelecidas como políticas para toda a organização.
- Há uma conscientização do risco de segurança cibernética no nível organizacional, mas não foi estabelecida uma abordagem válida para toda a organização.
- A avaliação do risco cibernético de ativos organizacionais e externos ocorre, mas não é tipicamente reproduzível ou recorrente.
- A organização colabora e recebe algumas informações de outras entidades.

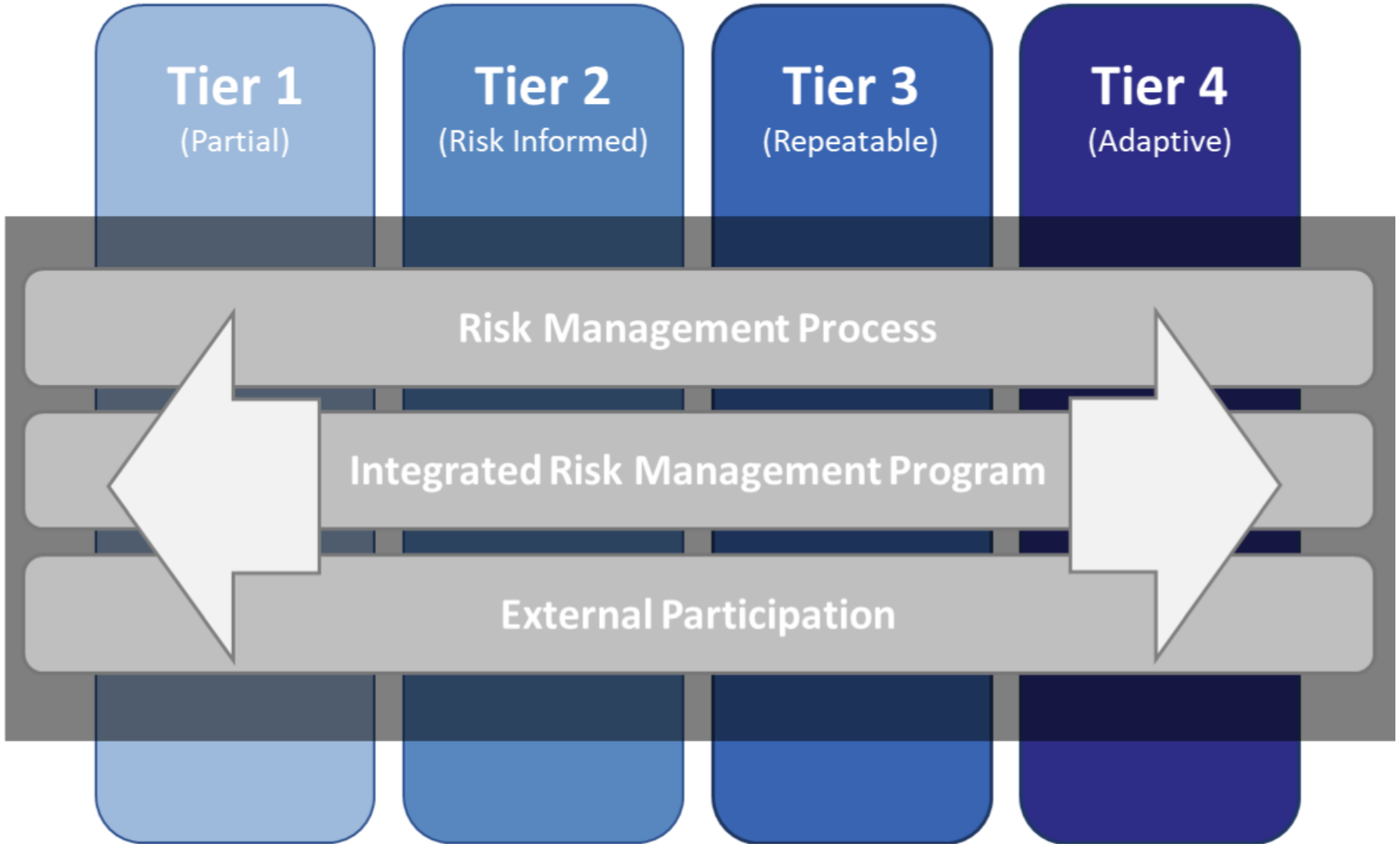
O NIST CSF: Camadas – Repetível

- As práticas de gerenciamento de risco da organização são formalmente aprovadas e expressas como política.
- Existem métodos consistentes para responder de forma eficaz às mudanças no risco.
- Existe uma abordagem para toda organização para gerenciar o risco de segurança cibernética.
- A organização monitora consistentemente e com precisão o risco de segurança cibernética nos ativos organizacionais.
- Executivos seniores asseguram a análise da segurança cibernética em todas as linhas de operação da organização.

O NIST CSF: Camadas – Adaptável

- A organização adapta suas práticas de cibersegurança com base em atividades anteriores e atuais, incluindo lições aprendidas e indicadores preditivos.
- A organização incorpora tecnologias e práticas avançadas de cibersegurança de forma adaptativa.
- O gerenciamento dos riscos de cibersegurança faz parte da cultura organizacional e evolui a partir da conscientização contínua das atividades em seus sistemas e redes.

O NIST CSF: Camadas



O NIST CSF: Camadas

- Vale notar que as camadas não representam necessariamente níveis de maturidade.
- As organizações precisam determinar sua camada desejada, que atenderá as metas organizacionais, reduzirá o risco de segurança a um nível aceitável e poderá ser implementada nos níveis financeiro e operacional.
- Não existe sistema ou rede 100% seguro.

O NIST CSF: Componentes - *Core*

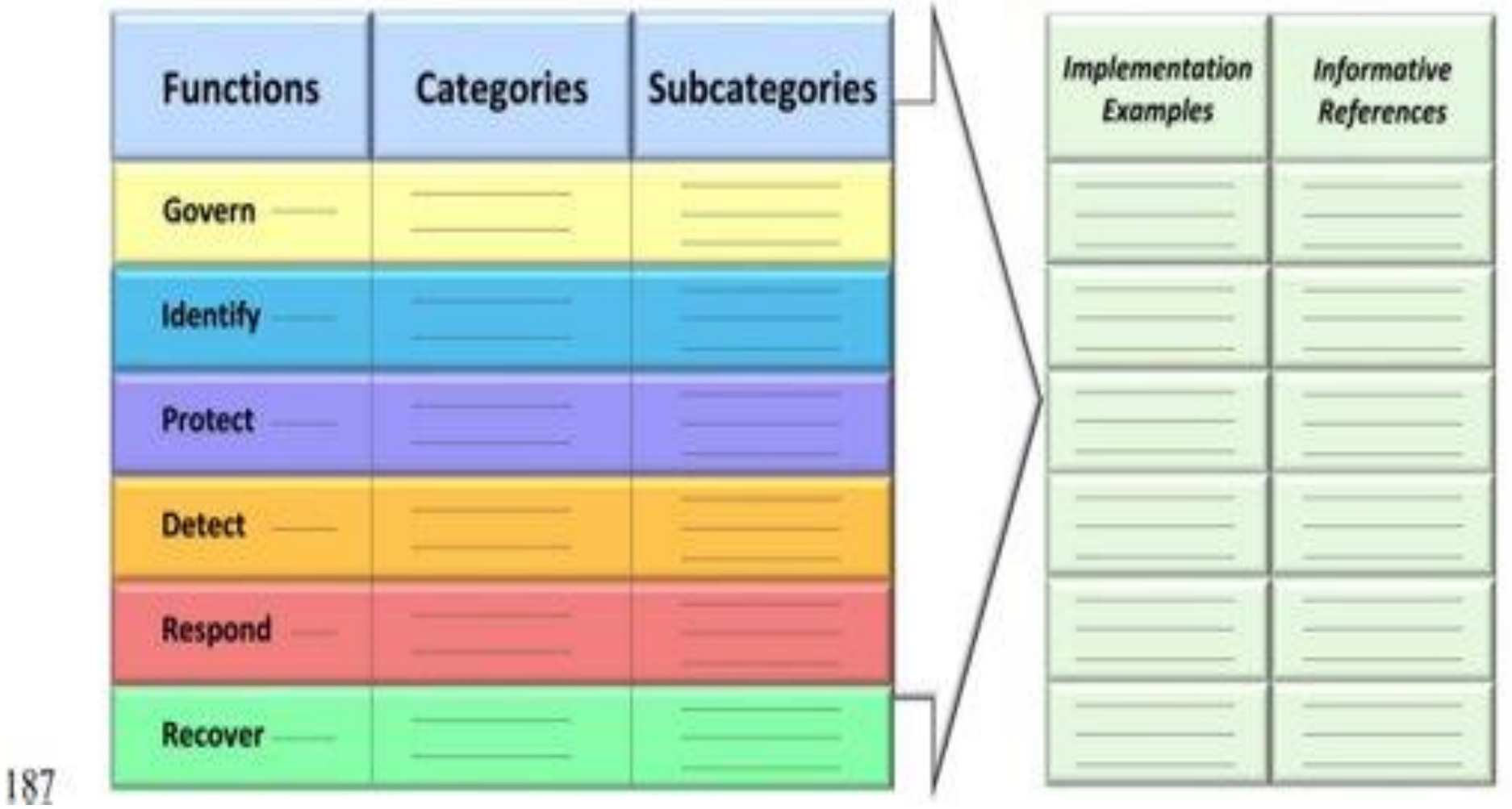
- O CSF *Core* foi desenvolvido para ajudar as organizações a definir quais atividades elas precisam realizar para atingir diferentes padrões de cibersegurança.

- Permite a comunicação entre equipes multidisciplinares utilizando uma linguagem simples e não necessariamente técnica.

O NIST CSF: Componentes - *Core*

- O *core* do *framework* consiste em **três partes**:
  - Funções (6): Governar, Identificar, detectar, proteger, responder e recuperar.
  - Categorias: Existem **22** categorias divididas nas cinco funções.
  - Subcategorias: Existem **108** subcategorias divididas nas **22** categorias.

O NIST CSF: Componentes - *Core*



Exercício

- Fotografia

FRAMEWORK	POLÍTICA ATUAL	PROCESSO INTERNO ATUAL	PRIORIDADE ALVO	**POLITICA ALVO, PROCESSO E PROCEDIMENTO**	**RESPONSABILIDADES ALVO**	**REFERÊNCIA INFORMATIVA**
Resposta	Sem politica	Padrão - resposta por ocorrência	Desenvolver politica de resposta	Relacionamento de equipe Treinamento de sala de guerra Gerencia de sala Governança de sala	Lista de funções e atribuições com tempo minimo e maximo de trabalho	Nist

O NIST CSF: Componentes - *Core*

- As **seis** funções se aplicam ao gerenciamento de riscos em geral.
- As categorias abrangem a amplitude dos objetivos de segurança cibernética.
- As subcategorias são declarações orientadas a resultados que fornecem considerações para criar ou melhorar um programa de segurança.

O NIST CSF: Componentes - *Core*

- Para cada subcategoria, é fornecido um recurso informativo que faz referência a seções específicas de outros padrões de segurança da informação, incluindo:
  - ISO 27001
  - COBIT
  - NIST SP 800-53 - Segurança e Privacidade
  - ANSI
  - CIS Controls
  - ISA-62443

O NIST CSF: Componentes - *Core*

daryus

NIST
CYBERSECURITY FRAMEWORK

GOVERNAR

CREDENCIADO
HSI INSTITUTE

IDESP
Instituto Daryus de Ensino Superior Paulista

Categorias da função **Governar**:

- **Contexto Organizacional (GV.OC)**
- **Estratégia de Gestão de Risco (GV.RM)**
- **Funções, responsabilidades e autoridades (GV.RR)**
- **Políticas (GV.PO)**
- **Supervisão (GV.OV)**
- **Gerenciamento de riscos da cadeia de suprimentos de segurança cibernética (GV.SC)**

O NIST CSF: Componentes - *Core*

- **Governar:** Como está desenhada a gerência do risco na companhia? O que está sendo visto e documentado?
- As organizações devem gerenciar e definir sua política de riscos e monitorar a estratégia do gerenciamento com foco na cibersegurança.
- A missão da empresa, bem como seus ativos devem estar bem definidos para todos os colaboradores, incluindo fornecedores.
- Requisitos regulatórios não podem ser esquecidos.

daryus

NIST
CYBERSECURITY FRAMEWORK

IDENTIFICAR

CREDENCIADO
HSI INSTITUTE

O NIST CSF: Componentes - *Core*

- **Identificar:** O que você tem? O que você está enfrentando?
- As organizações devem identificar seus dados e os dispositivos que armazenam, transmitem e processam informações.
- Você deve ter um inventário de dados, os dispositivos, os aplicativos e a infraestrutura subjacente que processa e armazena esses dados.
- Não se esqueça das versões e licenças de aplicativos e bibliotecas.

O NIST CSF: Componentes - *Core*

- **Identificar:** O que você tem? O que você está enfrentando?
- Se você sabe quais dados você tem, é possível identificar ameaças e vulnerabilidades no ambiente.
- Logo, você se concentra em proteger os ativos mais críticos ou o que é mais valioso para a sua organização.

- Categorias da função **Identificar**:
  - **Gestão de Ativos (ID.AM)**
  - **Avaliação de risco (ID.RA)**
  - **Melhoria (ID.IM)**

daryus

NIST
CYBERSECURITY FRAMEWORK

PROTEGER

CREDENCIADO
HSI INSTITUTE

O NIST CSF: Componentes - *Core*

- **Proteger:** Coloque medidas de proteção no lugar.
- Após saber o que você precisa proteger, é a hora de definir as medidas proativas e reativas para salvaguardar esses dados.
- Uma abordagem em camadas (defesa em profundidade) é fundamental para proteger as camadas de conectividade, aplicações e os próprios dispositivos.
- **Lembre-se:** Não basta apenas utilizar um *firewall*!

IDESP
Instituto Daryus de Ensino Superior Paulista

Categorias da função **Proteger**:

- **Gerenciamento de identidade, autenticação e controle de acesso (PR.AA)**
- **Conscientização e Treinamento (PR.AT)**
- **Segurança de Dados (PR.DS)**
- **Segurança da plataforma (PR.PS)**
- **Resiliência da infraestrutura tecnológica (PR.IR)**

daryus

NIST
CYBERSECURITY FRAMEWORK

DETECTAR

CREDENCIADO
HSI INSTITUTE

O NIST CSF: Componentes - *Core*

- **Detectar:** Monitore o seu ambiente.
- Nossa infraestrutura e aplicações sofrem mudanças com uma certa frequência. Portanto, monitore continuamente o ambiente.
- Isso permite que você detecte novos eventos e possíveis incidentes.
- É importante selecionar a melhor estratégia para o seu caso.
- Sempre avalie as ferramentas antes de usá-las. É uma ferramenta popular? A indústria está a utilizando?
- Também é sempre bom testar as ferramentas em uma *sandbox*.

O NIST CSF: *Overview* - Detectar

- Categorias da função **Detectar**:
  - **Monitoramento Contínuo (DE.CM)**
  - **Análise de Eventos Adversos (DE.AE)**

O NIST CSF: Componentes - *Core*

- **Detectar:** Monitore o seu ambiente.
- A detecção deve ser eficiente e eficaz. Imagine detectar um ataque DDoS em sua aplicação *web* apenas 30min, 1h ou até mesmo 2h depois de um incidente.
- Para algumas organizações, um *downtime* de poucos minutos pode ser crítico.
- Você não pode responder se não consegue detectar um ataque.
- Otimize e ajuste continuamente as tecnologias e processos que você possui.

daryus

NIST
CYBERSECURITY FRAMEWORK

RESPONDER

CREDENCIADO

HSI INSTITUTE

O NIST CSF: Componentes - *Core*

- **Responder:** Tenha um plano de resposta a incidentes.
- Tenha um plano de resposta formal e **testado**.
- Esse plano deve ser conhecido pela organização como um todo, seus *stakeholders* e respondentes.
- A detecção e resposta devem ser eficientes para que você possa voltar aos negócios o mais rápido possível.
- Assim como a detecção, o plano de resposta deve ser continuamente aprimorado.

O NIST CSF: *Overview* - Responder

- Categorias da função **Responder**:
  - **Gerenciamento de Incidentes (RS.MA)**
  - **Análise de Incidentes (RS.AN)**
  - **Relatório e comunicação de resposta a incidentes (RS.CO)**
  - **Mitigação de Incidentes (RS.MI)**

daryus

NIST
CYBERSECURITY FRAMEWORK

RECUPERAR

CREDENCIADO
HSI INSTITUTE

O NIST CSF: Componentes - *Core*

- **Recuperar:** Recupere em caso de incidentes e melhore.
- Por fim, mas não menos importante. A sua organização deve se recuperar em caso de violações.
- Embora nenhuma empresa queira passar por isso, é uma maneira de ver onde melhorias podem ser feitas.
- O *framework* permite lições aprendidas na vida real e reflete sobre como melhorar o processo geral.
- Da próxima vez, possivelmente o processo de resposta e recuperação será mais eficiente.

O NIST CSF: *Overview* - Recuperar

- Categorias da função **Recuperar**:
  - **Execução do Plano de Recuperação de Incidentes (RC.RP)**
  - **Comunicação de Recuperação de Incidentes (RC.CO)**

O NIST CSF: Componentes - *Profiles*

IDESP
Instituto Daryus de Ensino Superior Paulista

- O perfil representa o que a empresa tem hoje quando se fala em proteção de dados e onde ela quer chegar ou quais resultados ela quer ter.
- Cada organização tem um alinhamento exclusivo de requisitos, apetite de risco, recursos e objetivos que são pesados contra os resultados desejados do *Framework Core*.
- A organização pode observar lacunas em sua postura de cibersegurança, bem como identificar oportunidades de melhoria.

daryus

NIST
CYBERSECURITY FRAMEWORK

PERFIL

CREDENCIADO

HSI INSTITUTE

O NIST CSF: Como utilizar o guia?

IDESP
Instituto Daryus de Ensino Superior Paulista

- Organizações podem utilizar o guia como parte fundamental de seu processo sistemático para identificar, avaliar e gerenciar riscos de cibersegurança.
- Vale notar que o guia não foi projetado para substituir processos já existentes!
- Organizações podem utilizar seu processo atual e usar o guia para determinar e sanar lacunas em sua atual abordagem.

O NIST CSF: Componentes - *Profiles*

- Não existe uma maneira certa ou errada de se utilizar perfis.
- É apenas uma ferramenta para ajudar a otimizar o *framework* como um todo.
- Um bom método é mapear seus requisitos de cibersegurança, objetivos, métodos de operação e práticas atuais.
- Compare esse levantamento com as subcategorias fornecidas pelo *framework* para criar o perfil do seu estado atual.

O NIST CSF: Como utilizar o guia?

IDESP
Instituto Daryus de Ensino Superior Paulista

- O CSF é projetado para complementar operações existentes de negócios e segurança cibernética.
- Ele pode servir como base para um novo programa de cibersegurança ou como um mecanismo para melhorar um programa existente.
- O CSF pode ser aplicado em todas as fases do ciclo de vida do plano: design, desenvolvimento, implantação, operação e desativação.

O NIST CSF: Como utilizar o guia?

IDESP
Instituto Daryus de Ensino Superior Paulista

- Algumas etapas fundamentais para implantação do CSF:

- 1) **Priorize e determine o escopo:** Sua organização deve identificar seus objetivos de negócios e prioridades organizacionais. Isso permitirá que a organização tome decisões estratégicas sobre implementações de cibersegurança. O *framework* pode ser adaptado para suportar diferentes linhas de negócios ou processos dentro de uma organização.

O NIST CSF: Como utilizar o guia?

- Algumas etapas fundamentais para implantação do CSF:

- 2) **Oriente:** Uma vez que o escopo tenha sido definido, a organização deve identificar ameaças e vulnerabilidades aplicáveis aos sistemas e ativos.

O NIST CSF: Como utilizar o guia?

- Algumas etapas fundamentais para implantação do CSF:

- 3) **Crie uma avaliação atual:** Indique os resultados já obtidos e aponte as lacunas que precisam ser resolvidas.

O NIST CSF: Como utilizar o guia?

- Algumas etapas fundamentais para implantação do CSF:

- 4) **Realize uma avaliação de risco:** Identifique a probabilidade de uma ocorrência de segurança cibernética e o impacto que tal ocorrência poderia ter na organização. Vale notar que esse processo deve ser contínuo.

O NIST CSF: Como utilizar o guia?

IDESP
Instituto Daryus de Ensino Superior Paulista

- Algumas etapas fundamentais para implantação do CSF:

- 5) **Crie uma avaliação desejada:** Com qual maturidade você gostaria que a sua organização estivesse? Aponte todos os resultados desejados pela organização.

O NIST CSF: Como utilizar o guia?

- Algumas etapas fundamentais para implantação do CSF:

- 6) **Determine, analise e priorize as falhas:** É necessário analisar cautelosamente as vulnerabilidades encontradas, com o objetivo de definir os pontos onde serão concentrados mais esforços.

O NIST CSF: Como utilizar o guia?

- Algumas etapas fundamentais para implantação do CSF:

- 7) **Implemente um plano de ação:** Determine quais ações devem ser tomadas para tratar as lacunas identificadas nas etapas anteriores. Em seguida, ajuste suas práticas atuais de cibersegurança para alcançar a avaliação desejada.

Exercícios de fixação

1) Sobre o NIST, escolha a afirmação correta:

A. A função do NIST é prover a segurança dos Estados Unidos.

B. Sua missão é promover a inovação e competitividade industrial dos Estados Unidos.

C. É uma subdivisão da NSA.

D. Faz parte da OWASP Foundation.

Exercícios de fixação

2) Sobre as categorias de publicações do NIST, escolha a alternativa correta:

A. FIPS são *overviews* mensais das publicações e projetos do NIST.
B. ITL Bulletins são relatórios de pesquisa publicados pelo NIST.
C. SPs são especificações técnicas, guias e melhores práticas.
D. NISTIRs são padrões de segurança amplamente usados.

Exercícios de fixação

3) Quais as vantagens do CSF?

A. Facilita os processos de pentest e análise de vulnerabilidades.

B. Fornece uma linguagem comum e metodologia sistemática para gerenciar riscos de cibersegurança.

C. Protege nossas aplicações contra SQL Injection.

D. Evita fraudes bancárias.

Exercícios de fixação

4) Qual a ordem correta das camadas/níveis definidos pelo CSF?

A. Parcial, risco informado, repetível e adaptável.

B. Risco informado, repetível, parcial e adaptável.

C. Risco informado, parcial, repetívele adaptável.

D. Parcial, adaptável, risco informado e repetível.

Exercícios de fixação

5) Sobre a função **identificar**, escolha a alternativa correta:

A. Você precisa definir medidas proativas e reativas nessa etapa.

B. As organizações devem identificar seus dados e os dispositivos que armazenam, transmitem e processam dados.

C. Visa proteger os ativos menos críticos da organização.

D. Consegue mapear todas as vulnerabilidades existentes nos ativos.

Exercícios de fixação

6) Sobre a função **proteger**, escolha a alternativa correta:

A. Uma abordagem em camadas é fundamental para proteção dos ativos.

B. A utilização de um *firewall* resolve todos os problemas.

C. Visa proteger aplicações contra *Cross-Site Scripting*.

D. Se baseia em testes de intrusão em ambiente controlado.

Exercícios de fixação

7) Sobre a função **detectar**, escolha a alternativa correta:

A. O monitoramento do ambiente deve ser realizado mensalmente.

B. A análise de *logs* é ineficaz nessa etapa.

C. Precisamos monitorar continuamente nossas aplicações e infraestrutura, pois elas não são estáticas.

D. Serve para mitigar ataques de negação de serviço.

Exercícios de fixação

8) Sobre a função **responder**, escolha a alternativa correta:

A. O plano de resposta a incidentes deve ser testado na ocorrência de um incidente.

B. O plano de resposta deve ser mantido em sigilo.

C. O plano de resposta deve cobrir ataques de CSRF.

D. O plano de resposta deve ser continuamente aprimorado.

Exercícios de fixação

9) Sobre a função **recuperar**, escolha a alternativa correta:

A. Se seguirmos corretamente o *framework*, nunca chegaremos nessa função.

B. O *framework* permite lições aprendidas na vida real e reflete sobre como melhorar o processo geral.

C. Ataques de *ransomware* não podem ser solucionados sem o pagamento ao atacante.

D. Após a recuperação e aplicação das contramedidas, estaremos livres de ataques da mesma categoria.

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 3: GOVERNAR

CREDENCIADO
HSI INSTITUTE

Governar: Visão geral

Governar a estratégia de risco da organização, para oferecer um escopo ampliado de proteção de segurança cibernética para organizações de todos os tamanhos e em todos os setores.

“Governar” representa a sexta função, antecedendo “Identificar”, “Proteger”, “Detectar”, “Responder” e “Recuperar”.

Entre outras questões, as subcategorias incluem, especialmente, a ação do Board da companhia, e questiona como uma organização garante uma governança responsável e como um sistema de analítico que permita alcançar a responsabilização pelas ações dos líderes seniores, responsabilidade fiscal e planejamento sucessório, entre outras considerações.

O NIST CSF: *Overview* - Governar

- Categorias da função **Governar**:
  - **Contexto Organizacional (GV.OC)**
  - **Estratégia de Gestão de Risco (GV.RM)**
  - **Funções, responsabilidades e autoridades (GV.RR)**
  - **Políticas (GV.PO)**
  - **Supervisão (GV.OV)**
  - **Gerenciamento de riscos da cadeia de suprimentos de segurança cibernética (GV.SC)**

Governar: Contexto Organizacional (GV.OC)

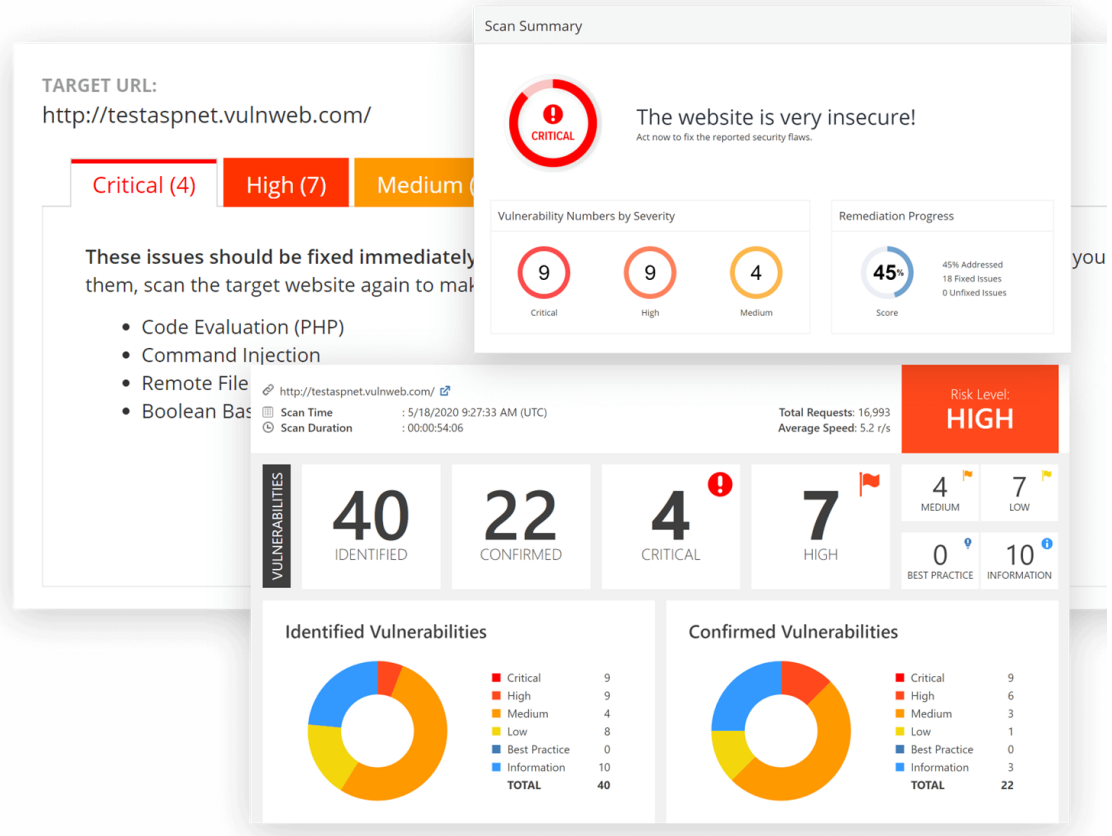
- Defina e comunique as prioridades organizacionais e o lugar da sua organização na infraestrutura crítica e setor industrial.
- Estabeleça prioridades para a missão organizacional, objetivos e atividades.
- Estabeleça dependências e funções críticas para entrega de serviços críticos.
- Estabeleça requisitos de resiliência para apoiar a prestação de serviços críticos em todas as condições operacionais.

Governar: Estratégia de Gestão de Risco (GV.RM)

- Análise de vulnerabilidades:
  - Processo de reconhecimento, análise e classificação de falhas de segurança.
  - A partir desse processo, é possível entender os pontos fracos de cibersegurança em nossas aplicações e sistemas.
  - Considerando o aumento dos ataques cibernéticos, é recomendável realizar esse processo com frequência.
  - É importante notar que podem ser encontrados falsos-positivos durante as análises, principalmente ao utilizar ferramentas automatizadas.
  - Portanto, sempre verifique com cautela os resultados!

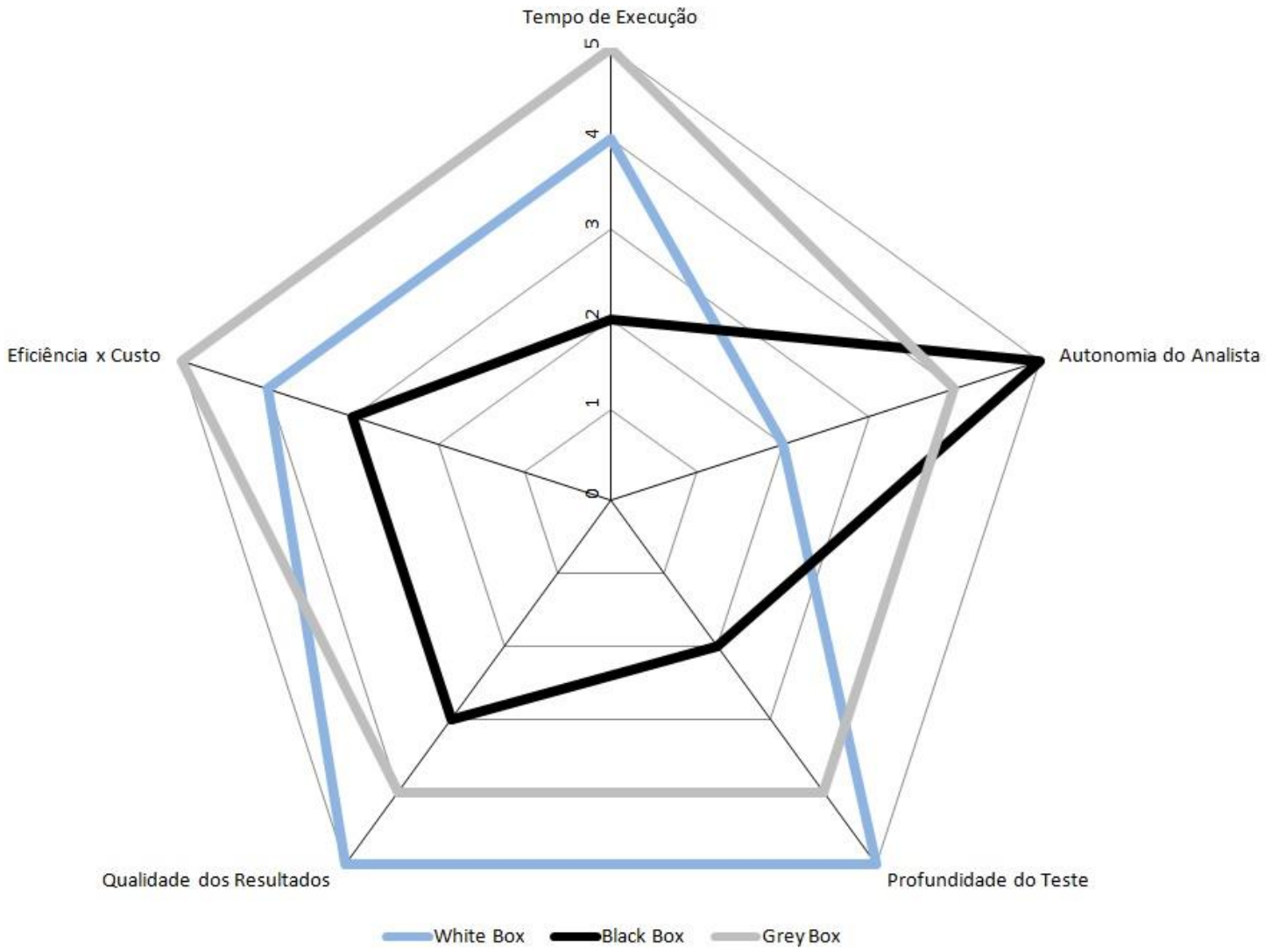
Governar: Estratégia de Gestão de Risco (GV.RM)

- Algumas ferramentas para análise de vulnerabilidades:
  - Acunetix
  - Nessus
  - OpenVAS
  - Nexpose
  - OWASP ZAP
  - Entre outras...



- Testes de intrusão:
  - Provê a visão de um atacante.
  - É fornecido um relatório com as técnicas ofensivas utilizadas e os resultados obtidos.
  - Visa eliminar os falsos-positivos que uma análise de vulnerabilidades pode gerar.
  - Existem três categorias:
    - Black-box: Nenhuma informação sobre a aplicação ou rede.
    - Gray-box: Informações parciais (e.g. credenciais de acesso).
    - White-box: Informação total e escopo bem definido.

Governar: Estratégia de Gestão de Risco (GV.RM)

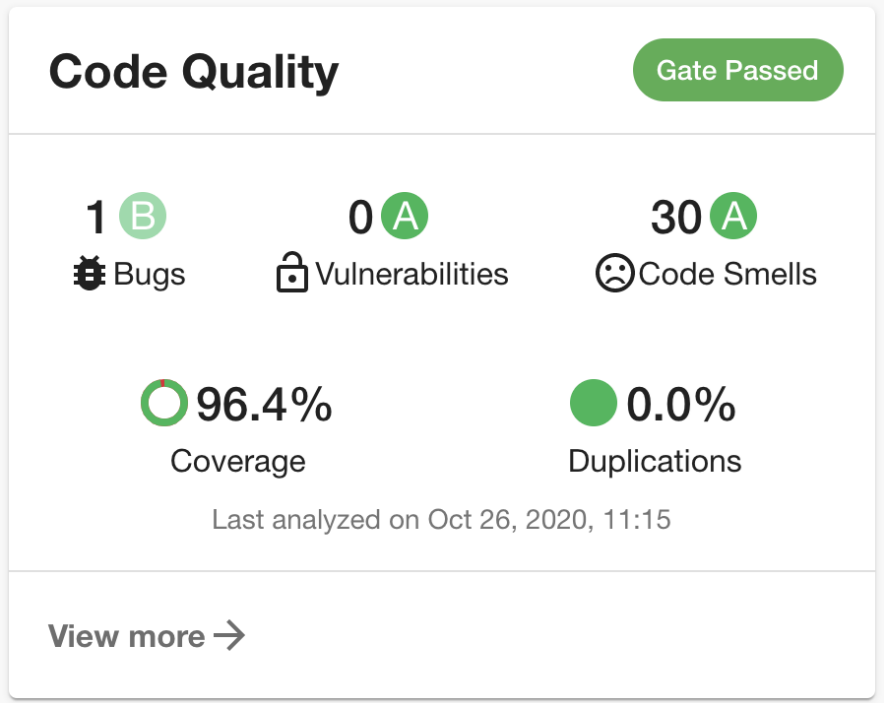


- Algumas ferramentas normalmente utilizadas em testes de intrusão:
  - Nmap
  - sqlmap
  - BurpSuite
  - Metasploit Framework
  - Exploits públicos (https://www.exploit-db.com / Searchsploit)

Governar: Estratégia de Gestão de Risco (GV.RM)

IDESP Instituto Daryus de Ensino Superior Paulista

- Algumas ferramentas para SAST:
  - Sonarqube
  - Veracode
  - Codacy
  - CodeFactor
  - Uma lista completa pode ser obtida em: https://owasp.org/www-community/Source_Code_Analysis_Tools



Governar: Estratégia de Gestão de Risco (GV.RM)

- SCA:
  - *Software Composition Analysis*.
  - Normalmente nunca escrevemos um *software* do zero. Ou seja, utilizamos componentes (bibliotecas, APIs, *frameworks*) de terceiros.
  - Muitas vezes esses componentes não foram construídos com segurança em mente.
  - Portanto, recomenda-se a verificação desses componentes em busca de vulnerabilidades.

- Algumas ferramentas para SCA:
  - OWASP Dependency Check
  - GitHub dependabot
  - Sonatype Nexus Platform
  - Entre outras...

Governar: Estratégia de Gestão de Risco (GV.RM)

IDESP Instituto Daryus de Ensino Superior Paulista

- Não se esqueça de verificar os riscos físicos!
- Seu datacenter tem os corretos mecanismos de redundância?
- As máquinas da sua corporação permitem que qualquer dispositivo USB seja inserido?
- O prédio da sua organização tem monitoramento por câmeras de segurança? Possui guardas?
- Como os funcionários se identificam? Crachás? *Smart cards*?

Governar: Estratégia de Gestão de Risco (GV.RM)

- Os processos de gerenciamento de risco devem ser estabelecidos, gerenciados e aprovados pelos *stakeholders* organizacionais.
- A tolerância ao risco organizacional deve ser determinada e claramente expressa.
- A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor.

Governar: Gerenciamento de riscos da cadeia de suprimentos de segurança cibernética (GV.SC)

- Os processos de gerenciamento devem ser identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.
- Fornecedores e parceiros terceirizados de sistemas devem ser identificados, priorizados e avaliados.
- Sempre formalize através de contratos os procedimentos para implementação de medidas apropriadas para atender aos objetivos do seu programa de segurança.

Governar: Gerenciamento de riscos da cadeia de suprimentos de segurança cibernética (GV.SC)

- Os fornecedores e parceiros tercerizados devem ser avaliados sistematicamente por meio de auditorias.
- Realize o planejamento e teste de resposta e recuperação com os prestadores de serviços terceirizados e também na própria organização.
- Não testar o seu plano de resposta pode causar problemas na prática.
- Avalie a evolução do seu plano de resposta.

Governar: Funções, responsabilidades e autoridades (GV.RR)

IDESP Instituto Daryus de Ensino Superior Paulista

- A política organizacional de cibersegurança em sua organização deve ser estabelecida e comunicada.
- As funções e responsabilidades de segurança cibernética devem ser coordenadas e alinhadas com funções internas e parceiros externos.
- Requisitos legais e regulamentares relativos à segurança cibernética devem ser compreendidos e gerenciados (e.g. proteção de dados e privacidade).

Governar: Funções, responsabilidades e autoridades (GV.RR)

IDESP Instituto Daryus de Ensino Superior Paulista

- A governança de dados é um dos pilares principais na transformação digital.
- Uma pesquisa realizada pelo PROCON/SP em julho de 2021 constatou que:
  - 65% dos brasileiros sequer sabiam o que era a LGPD.
  - 63% dos entrevistados sequer tomaram alguma atitude ao descobrir que foram vítimas de vazamentos de dados ou tentativas de golpes.
- Portanto, garanta juntamente com a equipe de cibersegurança que processos de proteção de dados estão sendo aplicados.

Governar: Políticas (GV.PO)

IDESP Instituto Daryus de Ensino Superior Paulista

- A política organizacional de cibersegurança em sua organização deve ser estabelecida e comunicada.
- As funções e responsabilidades de segurança cibernética devem ser coordenadas e alinhadas com funções internas e parceiros externos.
- Requisitos legais e regulamentares relativos à segurança cibernética devem ser compreendidos e gerenciados (e.g. proteção de dados e privacidade).

Governar: Políticas (GV.PO)

IDESP Instituto Daryus de Ensino Superior Paulista

- A governança de dados é um dos pilares principais na transformação digital.
- Uma pesquisa realizada pelo PROCON/SP em julho de 2021 constatou que:
  - 65% dos brasileiros sequer sabiam o que era a LGPD.
  - 63% dos entrevistados sequer tomaram alguma atitude ao descobrir que foram vítimas de vazamentos de dados ou tentativas de golpes.
- Portanto, garanta juntamente com a equipe de cibersegurança que processos de proteção de dados estão sendo aplicados.

Governar: Supervisão (GV.OV)

- Os resultados das atividades e do desempenho de gerenciamento de riscos de segurança cibernética em toda a organização são usados para informar, melhorar e ajustar a estratégia de gerenciamento de riscos

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 4: IDENTIFICAR

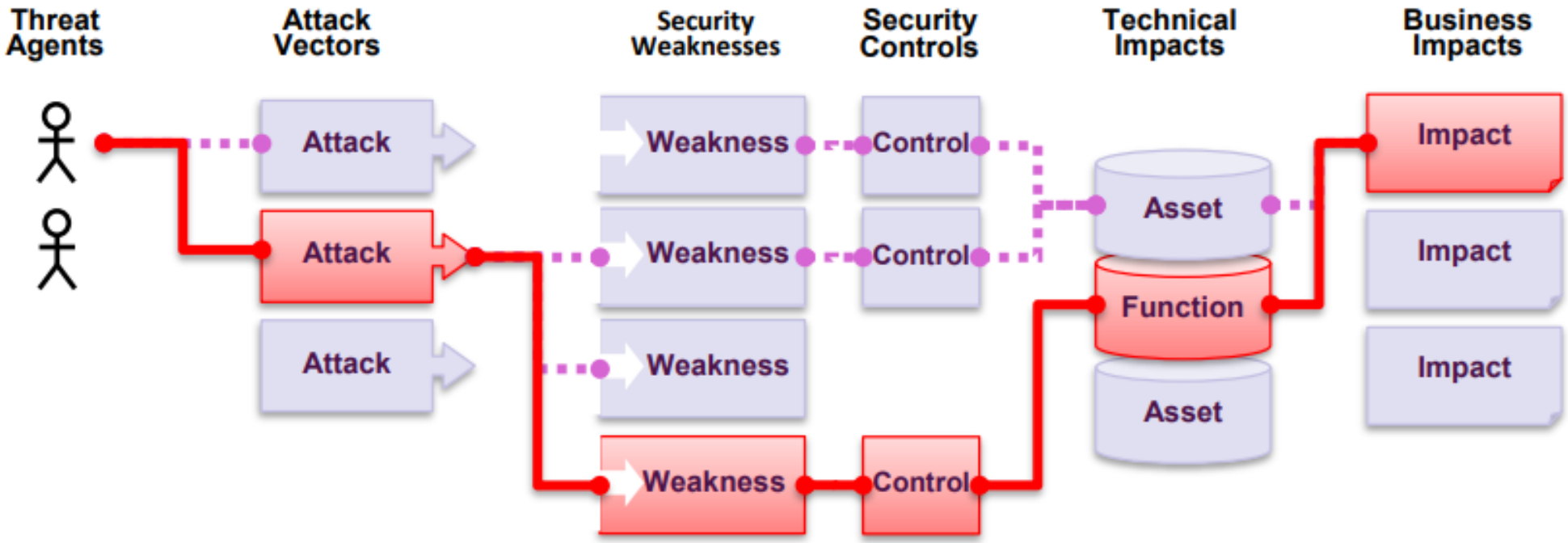
CREDENCIADO
HSI INSTITUTE

Identificar: Visão geral

- As atividades da função identificar são fundamentais para o uso eficiente do *framework*.
- Essa função abrange tópicos que permitem a uma organização desenvolver um entendimento organizacional para gerenciar riscos de segurança cibernética em sistemas, pessoas, ativos, dados e capacidades.
- Desse modo, é possível focar e priorizar seus esforços de uma forma consistente.

- Categorias da função **Identificar**:
  - **Gestão de Ativos (ID.AM)**
  - **Avaliação de risco (ID.RA)**
  - **Melhoria (ID.IM)**

Identificar: O que são riscos?



Identificar: Gestão de ativos (ID.AM)

- Dispositivos físicos e sistemas dentro da sua organização devem ser inventariados.
- Dispositivos?
  - Laptops, servidores, impressoras, ar-condicionado, *softwares* e serviços de terceiros (e.g. Gsuite, Office 365, Dropbox, entre outros).
- Ativos são geralmente utilizados para se realizar análise/avaliação de riscos.

Identificar: Gerenciamento de ativos (ID.AM)

- Como construir um inventário de ativos?
  - A melhor forma é “entrevistando” o responsável por cada departamento.
  - A partir disso, uma lista de todos os ativos que o departamento usa deverá ser fornecida.
  - Lembre-se de incluir uma lista de todos os *softwares* utilizados, além de documentos e pastas compartilhadas na rede.
  - A ISO 27001 não especifica como construir essa lista. Logo, você pode ter apenas o nome do usuário e dispositivo ou incluir mais detalhes.

Identificar: Gerenciamento de ativos (ID.AM)

- As comunicações e fluxos organizacionais também devem ser mapeados.
- Sempre mantenha um catálogo de qualquer serviço ou sistema externo que você estiver utilizando.
- Além disso, estabeleça funções e responsabilidades de cibersegurança para os colaboradores.
- Um programa de conscientização e boas práticas de utilização dos ativos pode auxiliar nesse processo.

Identificar: Gerenciamento de ativos (ID.AM)

IDESP
Instituto Daryus de Ensino Superior Paulista

- A manutenção e reparo de ativos organizacionais deve ser realizada e registrada.
- Pode-se realizar a manutenção remota de ativos.
- O acesso remoto deve ser registrado e controlado, visando impedir o acesso não autorizado.
  - Sempre utilize ferramentas aprovadas (e.g. OpenSSH).

Identificar: Gerenciamento de ativos (ID.RA)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Ativos são geralmente o elemento chave para identificação de riscos, juntamente com ameaças e vulnerabilidades.
- Se a sua organização não sabe quem é o responsável por cada ativo, o caos irá reinar.
- Um dos principais conceitos da ISO 27001 é justamente a definição dos proprietários de ativos e a designação de responsabilidades para eles quanto a proteção da tríade CID.

Identificar: Avaliação de risco (ID.RA)

- Vulnerabilidades devem ser identificadas e documentadas.
- Para isso, podemos utilizar ferramentas, testes manuais e automatizados para realizar:
  - Análise de vulnerabilidades.
  - Testes de intrusão.

Identificar: Melhorias (ID.IM)

- Melhorias nos processos, procedimentos e atividades organizacionais de gerenciamento de risco de segurança cibernética são identificadas em todas as funções da estrutura
  - Os planos de resposta a incidentes devem incorporar as lições aprendidas pela organização.
  - Estratégias de resposta devem ser atualizadas para refletir as lições aprendidas e novas políticas do negócio.

Identificar: Melhorias (ID.IM)

- Planos de recuperação devem incorporar as lições aprendidas.
- Estratégias de recuperação devem ser atualizadas.

Exercícios de fixação

1) São categorias da função identificar:

A. Governança, conscientização e treinamentos e segurança de dados.

B. Gerenciamento de ativos, gerenciamento de risco e Implementação de gerenciamento de risco cibernético.

C. Anomalias e eventos, processos de detecção e monitoramento contínuo.

D. Análise, mitigação e planejamento de respostas.

Exercícios de fixação

2) A gestão de ativos visa alcançar e manter a proteção adequada dos ativos da organização, sendo que:

A. A implementação de controles específicos pode ser delegada pelo proprietário, passando a responsabilidade pela proteção destes ativos a quem assumiu a sua implementação.

B. Os níveis de proteção devem ser iguais para todos os ativos, considerando-se que todos eles são importantes para a organização.

C. A proprietário do ativo deve ser responsável por definir e, periodicamente, analisar criticamente as classificações e restrições ao acesso aos ativos importantes, levando em conta as políticas de controle de acesso aplicáveis.

D. É facultativo a fornecedores e terceiros seguir as regras para o uso permitido de informações e de ativos associados aos recursos de processamento da informação, porém, é obrigatório aos funcionários.

Exercícios de fixação

3) Sobre o processo de definição de um inventário para o gerenciamento de ativos, está incorreta:

A. A melhor forma é entrevistar o responsável por cada departamento.

B. É importante incluir softwares e pastas compartilhadas na rede.

C. Não precisamos mapear fluxos organizacionais.

D. Precisamos mapear sistemas de terceiros.

Exercícios de fixação

4) Qual dos seguintes itens busca proporcionar clareza e transparência nos serviços de TI?

A. Gerenciamento da capacidade.

B. Governança.

C. Desenho de serviço.

D. Gerenciamento do nível de serviço.

Exercícios de fixação

6) Sobre testes de intrusão, escolha a alternativa correta:

A. Testes white-box geram relatórios menos profundos devido ao escopo limitado.

B. Testes gray-box são testes onde o atacante tem visão completa sobre a arquitetura do sistema.

C. A melhor eficiência x custo é obtida nos testes gray-box.

D. Testes black-box são os menos demorados, visto que apenas URLs são normalmente informadas.

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 5: PROTEGER

CREDENCIADO
HSI INSTITUTE

Proteger: Visão geral

- Tem como objetivos o desenvolvimento e implementação das proteções necessárias para garantir a prestação de serviços críticos.
- Fornece apoio à capacidade de limitar ou conter o impacto de um possível incidente de cibersegurança.

IDESP
Instituto Daryus de Ensino Superior Paulista

- Categorias da função **Proteger**:
  - **Gerenciamento de identidade, autenticação e controle de acesso (PR.AA)**
  - **Conscientização e Treinamento (PR.AT)**
  - **Segurança de Dados (PR.DS)**
  - **Segurança da plataforma (PR.PS)**
  - **Resiliência da infraestrutura tecnológica (PR.IR)**

Proteger: Gerenciamento de identidade, autenticação e controle de acesso (PR.AA)

IDESP Instituto Daryus de Ensino Superior Paulista

- Autenticação x Autorização:
- **Autenticação:** Processo de reconhecer a identidade de um usuário.
  - Nome de usuário e senha.
  - E-mail e senha.
  - CPF e senha.
- **Autorização:** Níveis de privilégio que o usuário terá no sistema.
  - Usuário comum.
  - Gerente.
  - Administrador de rede.

Proteger: Controle de acesso (PR.AA)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Identidades e credenciais devem ser emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.
- O acesso físico aos dispositivos deve ser gerenciado e protegido.
- O acesso remoto deve ser gerenciado (RDP, SSH, etc).
- Permissões de acesso e autorizações devem ser gerenciadas.
- Sempre aplique o princípio do menor privilégio e divisão de tarefas.

Proteger: Controle de acesso (PR.AA)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Menor privilégio:
  - Um usuário ou processo deve ter apenas as permissões necessárias para realizar a sua tarefa, nada mais.
  - Problemas pela falta do menor privilégio podem ser catastróficos.

- Divisão de tarefas:
  - A conclusão de uma operação depende da finalização bem-sucedida de uma ou mais tarefas.

Proteger: Controle de acesso (PR.AA)

- A integridade da rede deve ser protegida.
  - Várias ferramentas podem nos auxiliar nisso. Por exemplo: IDS/IPS, ferramentas para análise de *logs*, antivirus...
- As identidades devem ser revisadas, vinculadas a credenciais e confirmadas em interações.
  - Nunca se esqueça de desativar contas de ex-funcionários.

Proteger: Controle de acesso (PR.AA)

- Usuários, dispositivos e outros recursos devem ser autenticados de acordo com o risco da transação.
- Considere utilizar 2FA ou MFA.
  - Muitas invasões a contas de usuários poderiam ser evitadas através desse simples mecanismo.
- Sempre exija que o usuário confirme a sua senha antes de realizar ações críticas.

Proteger: Conscientização e treinamento (PR.AT)

- Todos os funcionários devem ser informados a respeito de treinamentos.
- Os usuários privilegiados devem compreender suas funções, responsabilidades e a importância dos controles de cibersegurança.
- *Stakeholders* terceirizados devem ter a mesma visão dos usuários da empresa a respeito dos controles de cibersegurança.
- Executivos devem compreender suas funções, responsabilidades e assegurar que os devidos controles de segurança cibernética estão sendo aplicados.

Proteger: Conscientização e treinamento (PR.AT)

- O papel dos profissionais de cibersegurança em programas de conscientização e treinamento é fundamental para a correta manutenção dos controles de cibersegurança aplicados.
- Nesse contexto, podemos propor e executar treinamentos de:
  - Desenvolvimento seguro.
  - Segurança de aplicações.
  - Conscientização contra ataques de *phishing*.
  - Entre outros...

Proteger: Conscientização e treinamento (PR.AT)

- Em caso de testes de *phishing*, lembre-se de estabelecer um escopo com os seus superiores.
- Sempre avise às vítimas que elas caíram em um *phishing* simulado.
  - Também é importante solicitar a elas que não divulguem essa informação.
  - Isso pode comprometer os resultados da campanha.

Proteger: Segurança de dados (PR.DS)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Os dados em armazenamento e em trânsito devem ser protegidos.
- Armazenamento:
  - Criptografia de arquivos.
  - Armazenamento de senhas em bancos: PBKDF2, bcrypt, scrypt.
  - *k-anonymity*.
- Transporte:
  - TLS versão 1.2 ou superiores.
  - Algoritmos como o SSL e versões do TLS anteriores à 1.2 já são considerados inseguros.

Proteger: Segurança de dados (PR.DS)

- Os ativos devem ser formalmente gerenciados durante a remoção, transferências e disposição.
- Sempre tenha redundâncias adequadas para garantir a disponibilidade dos seus sistemas e dados que eles precisam durante uma operação de troca.
- É de extrema importância separar os ambientes de desenvolvimento dos de produção.
  - Além disso, tenha em mente que todas as credenciais devem mudar em ambiente de produção, seguindo as melhores práticas estabelecidas.

Proteger: Segurança de dados (PR.DS)

- Tenha proteções contra vazamentos de dados.
- Não há um processo de proteção padrão definido para qualquer aplicação.
- Organizações possuem *stacks* diversificadas.
- O ideal é realizar periodicamente a análise de vulnerabilidades, identificando todos os dados críticos que nossos sistemas utilizam e aplicar as corretas contramedidas.

Proteger: Segurança da Plataforma (PR.PS)

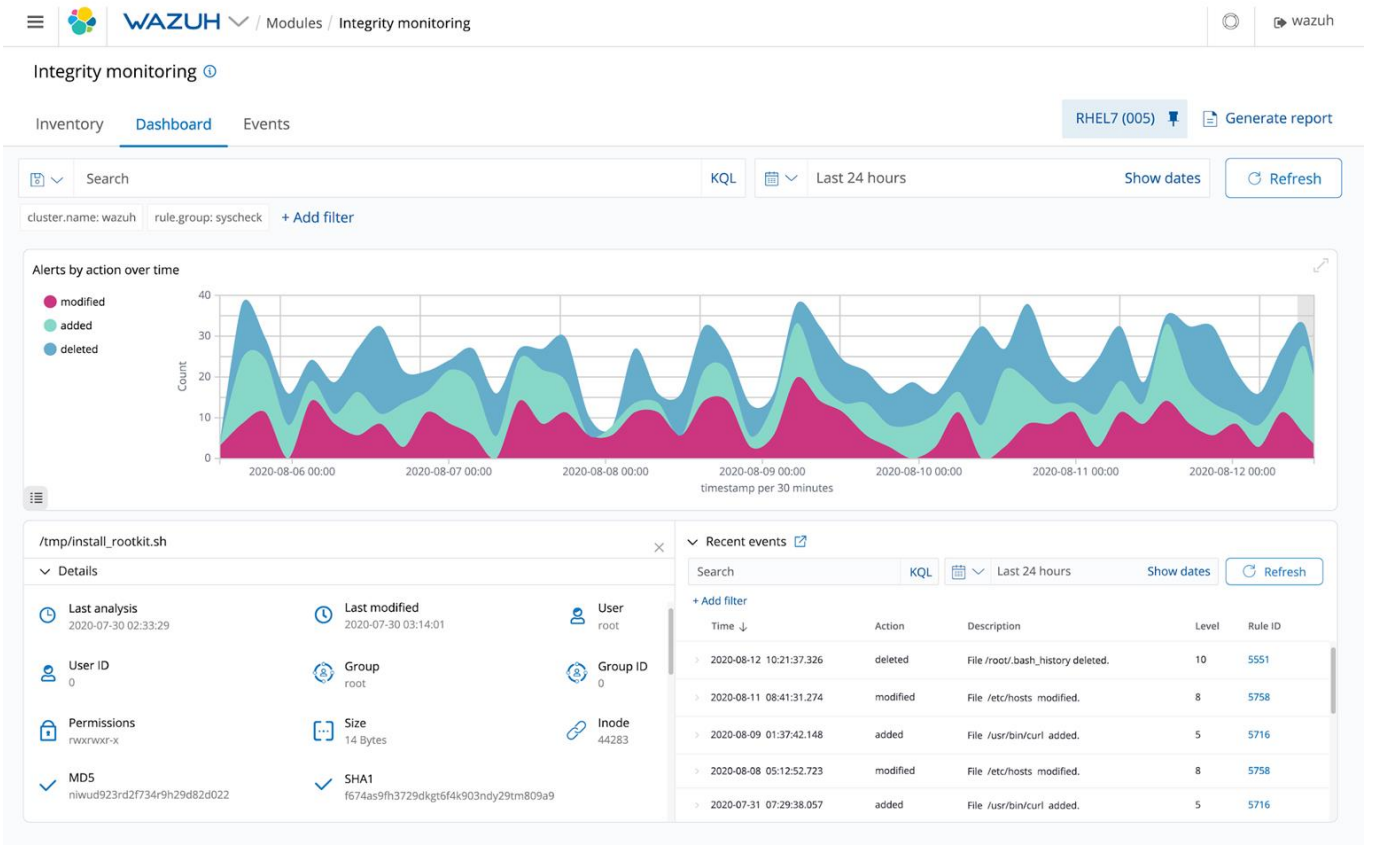
- Os registros de auditoria devem ser:
  - Determinados.
  - Documentados.
  - Implementados.
  - Revisados de acordo com a política.
- As mídias removíveis devem ser protegidas e seu uso deve ser restrito de acordo com a política da corporação.

Proteger: Segurança da Plataforma (PR.PS)

- O princípio da menor funcionalidade deve ser incorporado através da configuração dos sistemas para fornecer apenas recursos essenciais.
- Redes de comunicação e de controle devem ser devidamente protegidas.
- Mecanismos devem ser implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas.

Proteger: Algumas ferramentas

- Wazuh: Excelente solução para monitoramento de comportamentos na rede.
- Algumas funcionalidades:
  - Detecção de intrusão.
  - Monitoramento de arquivos.
  - Segurança de *containers*.
  - Segurança em *cloud*.
  - Requisitos de *compliance*.



Proteger: Algumas ferramentas

- Yubikey: Dispositivo para 2FA.

Proteger: Segurança da plataforma (PR.PS)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Menor funcionalidade.
  - Usuários devem ter privilégio mínimo em nossos sistemas.
  - Isso significa que eles só podem acessar páginas, rotas e funções que os mesmos possuem autorização.
  - Sempre verifique sua implementação para averiguar se um correto controle de acesso está sendo realizado.

Proteger: Segurança da plataforma (PR.PS)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Backups de informações devem ser realizados, conservados e testados.
  - Sempre tenha mais de um backup.
  - De preferência em máquinas com localizações distintas.
  - Ambientes em cloud, como o AWS, facilitam bastante esse trabalho e possuem preços acessíveis.
  - Sempre verifique a integridade dos logs e backups através de *hashes*.
- Dados eventualmente podem ser destruídos de acordo com a política de retenção da empresa.

Proteger: Segurança da plataforma (PR.PS)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Os processos de proteção de dados devem ser periodicamente revisados e aperfeiçoados.
- A eficácia das tecnologias de proteção é compartilhada entre membros da organização e parceiros.
- Planos de resposta e recuperação em vigor precisam ser testados e gerenciados.

Proteger: Segurança da plataforma (PR.PS)

- A segurança cibernética deve estar incluída nas práticas de recursos humanos.
- Um plano de gerenciamento de vulnerabilidades deve ser desenvolvido e implementado.

Proteger: Segurança da plataforma (PR.PS)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Ciclo de vida de desenvolvimento seguro.
- Também chamado de SDLC ou SSDLC em inglês.
- Criado pela Microsoft e publicado em 2008.
- Visa garantir a aplicação de controles que tornem um software seguro o suficiente para ser usado com um nível de risco aceitável.
- Dividido em 12 fases principais, sendo a 1ª o treinamento de segurança para desenvolvedores.

Proteger: Resiliência da infraestrutura tecnológica (PR.IR)

IDESP Instituto Daryus de Ensino Superior Paulista

- Fases do SDLC:

Fornecer treinamentos

Definir requisitos de segurança

Definir métricas e compliance

Realizar modelagem de ameaças

Proteger: Resiliência da infraestrutura tecnológica (PR.IR)

IDESP Instituto Daryus de Ensino Superior Paulista

- Fases do SDLC:

Estabelecer requisitos de design

Definir e usar padrões de criptografia

Gerenciar o risco de segurança do uso de componentes de terceiros

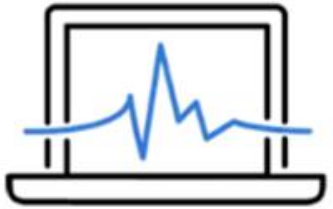
Usar ferramentas aprovadas

Proteger: Resiliência da infraestrutura tecnológica (PR.IR)

- Fases do SDLC:

Executar testes de segurança de análise estática (SAST)

Executar testes de segurança de análise dinâmica (DAST)



Realizar testes de invasão

Estabelecer um processo padrão de resposta a incidentes

Exercícios de fixação

1) São categorias da função proteger:

A. Controle de acesso, Segurança de dados, Infraestrutura e resiliência tecnológica, ambiente cibernético e treinamento.

B. Tecnologia de proteção, *pentest* e controle de acesso.

C. Tecnologia de proteção, controle de acesso e análise de vulnerabilidades.

D. Autorização, autenticação e controle de fluxo.

Exercícios de fixação

2) Qual alternativa melhor descreve a responsabilização no controle de acesso?

A. Método que o indivíduo utiliza para solicitar acesso ao sistema.

B. Processo de determinar se um usuário está aprovado para acessar determinados recursos.

C. Validação ou prova de que o indivíduo que recebeu acesso foi o mesmo que o solicitou.

D. Manter informações para auditoria.

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 6: DETECTAR

CREDENCIADO
HSI INSTITUTE

Detectar: Visão geral

- Tem como principais objetivos o desenvolvimento de implantação de atividades necessárias para identificar a ocorrência de um incidente de cibersegurança.
- Permite a descoberta oportuna de eventos críticos de cibersegurança.

IDESP
Instituto Daryus de Ensino Superior Paulista

- Categorias da função **Detectar**:
  - **Monitoramento Contínuo (DE.CM)**
  - **Análise de Eventos Adversos (DE.AE)**

Detectar: Monitoramento contínuo de segurança (DE.CM)

IDESP
Instituto Daryus de Ensino Superior Paulista

- A rede da corporação deve ser monitorada para detectar potenciais incidentes de cibersegurança.
- Ademais, o ambiente físico também deve ser monitorado.
- Lembre-se de monitorar as ações dos colaboradores.
- Atividades de provedores de serviços externos devem ser monitoradas para detectar possíveis eventos de cibersegurança.

Detectar: Monitoramento contínuo de segurança (DE.CM)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Código malicioso deve ser detectado.
  - Ferramentas como o ClamAV e Yara podem nos auxiliar nisso.
- Código malicioso em dispositivos móveis também deve ser detectado.
- O monitoramento de colaboradores não autorizados, conexões, dispositivos e *software* deve ser realizado.
- Varreduras por vulnerabilidades devem ser realizadas periodicamente.

Detectar: Análise de eventos adversos (DE.AE)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Estabeleça uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas.
  - Isso permite que identifiquemos ações suspeitas através de técnicas heurísticas.
- Os eventos devem ser analisados para compreender os alvos e métodos de ataque.
  - O uso de um *honeypot* pode ser bastante útil para gerar estudos e indicadores de comprometimento.

Detectar: Análise de eventos adversos (DE.AE)

- Dados da ocorrência devem ser coletados e correlacionados a partir de várias fontes de informação.
  - Muitas informações também podem ser coletadas através de técnicas de OSINT (sites de *pastes*, *deep web*, entre outros).
- Sempre classifique o impacto dos eventos.
  - Informacionais, risco baixo, risco médio, risco alto, risco crítico.
  - O *Common Vulnerability Scoring System* (CVSS) é um padrão da indústria gratuito e aberto para avaliar a gravidade das vulnerabilidades de segurança em sistemas.

Detectar: Análise de eventos adversos (DE.AE)

- Papéis e responsabilidades para detecção devem ser bem definidos para garantir a prestação de contas.
- Atividades de detecção devem cumprir todos os requisitos aplicáveis.
- Os processos de detecção devem ser testados.
- Informações de detecção de incidentes devem ser comunicadas.
- Processos de detecção devem ser continuamente aperfeiçoados.

Detectar: Algumas ferramentas

- Honeypots: Simulam ambientes. Logo, podemos coletar informações sobre as técnicas e ferramentas mais utilizadas pelos atacantes.
- Tipos de honeypot:
  - Alta interatividade: Usa serviços reais instalados. É importante manter o isolamento. Informações tendem a ser bem detalhadas.
  - Média interatividade: Simula alguns serviços como FTP ou servidor web. As informações geradas podem não ser muito detalhadas.
  - Baixa interatividade: Simula serviços básicos de rede. Informações tendem a ser muito escassas. Além disso, é muito mais fácil de ser detectado.

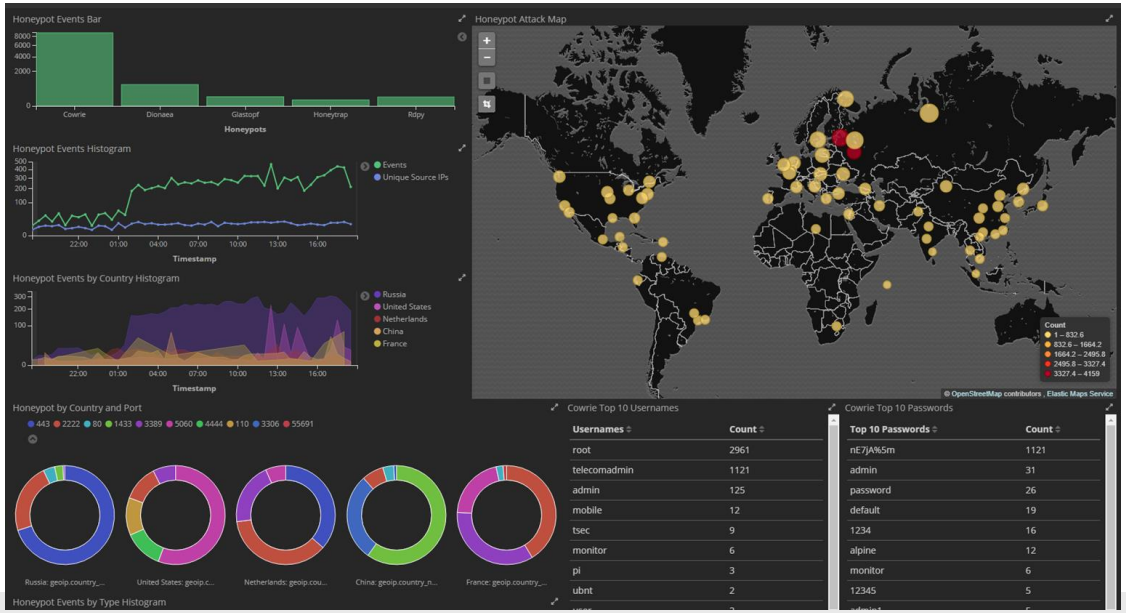
Detectar: Algumas ferramentas

IDESP
Instituto Daryus
de Ensino Superior
Paulista

- Muitas das ferramentas que estudamos no módulo anterior também podem ser utilizadas para detecção de ameaças, como:
  - Wazuh.
  - ELK Stack.
  - Snort.
  - ModSecurity.

Detectar: Algumas ferramentas

- Honeypots mais utilizados:
  - Cowrie: Para telnet e SSH.
  - Dionaea: Consegue simular serviços como FTP, HTTP, MySQL e SMB.
  - Dockpot: Utiliza Docker para criar um *honeypot* de SSH.
  - Glastopf: Muito utilizado para aplicações web.



Detectar: Algumas ferramentas

- Cuckoo sandbox: Uma das ferramentas mais renomadas para análise de malware. Algumas funções:
  - Análise de arquivos (executáveis, PDFs, e-mails) e websites.
  - Enumeração de chamadas a APIs.
  - Análise de tráfego.
  - Análise da memória volátil (através do Volatility).

Detectar: Algumas ferramentas

- YARA: Ferramenta open-source que auxilia no processo de detecção e classificação de *malware*.
- Permite a configuração de regras para identificação de novos binários maliciosos.
- Centenas de regras estão disponíveis publicamente.
- Desenvolvida pela VirusTotal.

Detectar: Algumas ferramentas

- ClamAV: Antivírus gratuito e open-source para sistemas Linux.

Exercícios de fixação

1) São categorias da função detectar:

A. Análise de Eventos Adversos e monitoramento contínuo.

B. SDLC, menor privilégio e segurança de dados.

C. Tecnologia de proteção, eventos e manutenção.

D. Análise de eventos, monitoramento contínuo e processos de detecção.

Exercícios de fixação

2) Na administração de segurança, os arquivos de log de um sistema estão relacionados a qual propósito?

A. Auditoria de segurança.
B. Integridade nas transações.
C. Não repúdio.
D. Garantia de disponibilidade dos serviços.
E. Confiabilidade das transações.

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 7: RESPONDER

CREDENCIADO
HSI INSTITUTE

Responder: Visão geral

- Tem como objetivos o desenvolvimento e implementação de atividades apropriadas para agir contra um incidente de cibersegurança detectado.
- Suporta a capacidade de conter o impacto de um possível incidente de cibersegurança.

IDESP
Instituto Daryus de Ensino Superior Paulista

- Categorias da função **Responder**:
  - **Gerenciamento de Incidentes (RS.MA)**
  - **Análise de Incidentes (RS.AN)**
  - **Relatório e comunicação de resposta a incidentes (RS.CO)**
  - **Mitigação de Incidentes (RS.MI)**

Responder:Gerenciamento de Incidente (RS.MA)

IDESP
Instituto Daryus de Ensino Superior Paulista

- O plano de resposta a incidentes deve ser executado durante ou depois de um incidente.
- Os funcionários devem conhecer seus papéis em um plano de resposta a incidentes.

Responder: Análise de Incidente (RS.AN)

- Sistemas de detecção de intrusão devem gerar alertas e esses alertas precisam ser analisados pela equipe responsável.
- É necessário compreender o impacto do incidente.
  - Indisponibilidade dos sistemas?
  - Comprometimento dos dados?
  - Vazamento de informações pessoais?

Responder: Análise de Incidentes (RS.AN)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Realize investigações e análises nos logs gerados pelos seus sistemas de detecção e prevenção de intrusões.
- Categorize os incidentes de forma consistente com os planos de resposta.

Responder: Relatório e comunicação de resposta a incidentes(RS.CO)

IDESP Instituto Daryus de Ensino Superior Paulista

- Os incidentes devem ser informados de acordo com os critérios estabelecidos.
- As informações devem ser compartilhadas de acordo com os planos de resposta.
- A coordenação com os *stakeholders* deve ocorrer de acordo com os planos de resposta.
- É recomendado compartilhar as informações sobre incidentes com os *stakeholders* externos para uma conscientização situacional mais ampla sobre segurança cibernética.

Responder: Mitigação de Incidentes (RS.MI)

IDESP
Instituto Daryus de Ensino Superior Paulista

- Incidentes precisam ser contidos e mitigados.
- Vulnerabilidades identificadas recentemente devem ser mitigadas e documentadas.
- Contas suspeitas devem ser desativadas e mantidas o tempo suficiente para uma análise forense.
- Sempre mantenha seus sistemas de antivírus atualizados com as últimas bases de dados.

Exercícios de fixação

1) São categorias da função responder:

   A. Gerenciamento de Incidente, Análise de incidente, Relatório de resposta a incidente , Mitigação de Incidentes.

   B. Planejamento de respostas, mitigação e melhorias.

   C. Aplicação de contra-medidas, mitigação e monitoramento contínuo.

   D. Melhorias, controle de acesso e comunicações.

Exercícios de fixação

2) Após um incidente de segurança de informação ser tratado, um trabalho forense deverá ser realizado sobre os originais do material de evidência mitigar o risco.

A. Correto.

B. Errado.

daryus

NIST
CYBERSECURITY FRAMEWORK

Módulo 8: RECUPERAR

CREDENCIADO
HSI INSTITUTE

Recuperar: Visão geral

- Tem como objetivos o desenvolvimento e implementação de atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança.

IDESP
Instituto Daryus de Ensino Superior Paulista

- Categorias da função **Recuperar**:
  - **Execução do Plano de Recuperação de Incidentes (RC.RP)**
  - **Comunicação de Recuperação de Incidentes (RC.CO)**

Recuperar: Execução do Plano de Recuperação de Incidentes (RC.RP)

IDESP
Instituto Daryus de Ensino Superior Paulista

- O plano de recuperação deve ser executado durante ou após um incidente de segurança cibernética.

Recuperar: Comunicações (RC.CO)

- As relações públicas devem ser gerenciadas.
- A reputação da organização deve ser reparada após incidentes.
- As atividades de recuperação devem ser comunicadas aos *stakeholders* internos e externos, bem como às equipes executivas e de gestão.

Referências

1. https://www.nist.gov/cyberframework

2. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

3. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

4. https://owasp.org

5. https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf

6. https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

7. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf

8. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

9. https://www.nist.gov/profiles-0

10. https://www.cisa.gov/resources-tools/all-resources-tools

11. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started

daryus

NIST
CYBERSECURITY FRAMEWORK

EXERCÍCIO - SEQUESTRO DE TORRES

CREDENCIADO
HSI INSTITUTE

daryus

NIST
CYBERSECURITY FRAMEWORK

AVALIAÇÃO

CREDENCIADO
HSI INSTITUTE