Framework de Segurança Cibernética

Força Tarefa Temporária de Segurança Cibernética

Associadas da ABRATE

ARGO

CEEE GERAÇÃO E TRANSMISSÃO

celeoredes

CELG

CEMIG

Chesf

COPEL

isa CTEEP

Eletrobras Eletronorte

Eletrobras Eletrosul

ENGIE

evoltz

FC empreendimentos e participações

FURNAS

ITAIPU BINACIONAL

QUANTUM

NEOENERGIA

STATE GRID BRAZIL HOLDING S.A. 国家电网巴西控股公司

Sterlite Power

taesa

ABRATE

AGENDA

- Motivação
- Objetivos
- Framework ABRATE
- Componentes do Framework
- Metodologia de Implementação
- Modelo de Maturidade e Mapeamento para o Framework
- Conclusões
- Trabalhos Futuros

Motivação

- Crescente dependência tecnológica no ambiente operacional.
- Regulamentação incipiente do setor: “Recursos tecnológicos para proteção contra ataques cibernéticos na rede de supervisão e controle dos centros de operação” (Submódulo 10.14 ONS).
  - Minuta de Procedimento de Rede de Segurança Cibernética
- Crescimento de ameaças cibernéticas no cenário internacional.
- Compartilhamento de Instalações.
- Falta de parâmetro para comparação entre as empresas.

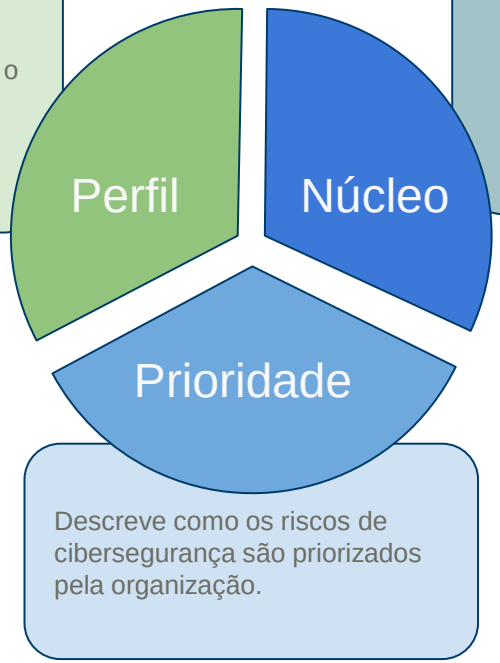
Objetivos

- Criar um Framework para melhoria da Segurança Cibernética nas empresas associadas da ABRATE.
- Permitir a implantação pelas empresas independentemente do atual nível de segurança, capacidade operacional ou recursos financeiros.
- Servir como sugestão de modelo de segurança cibernética para o Setor Elétrico nacional.

Framework ABRATE

Baseado na implementação do DOE do framework do NIST

O Perfil pode ser usado para identificar oportunidades para melhorar a posição de segurança cibernética, comparando um Perfil Atual com um Perfil Alvo. Perfis fornecem um roteiro para reduzir o risco em segurança cibernética de acordo com as práticas do negócio e boas práticas de mercado.

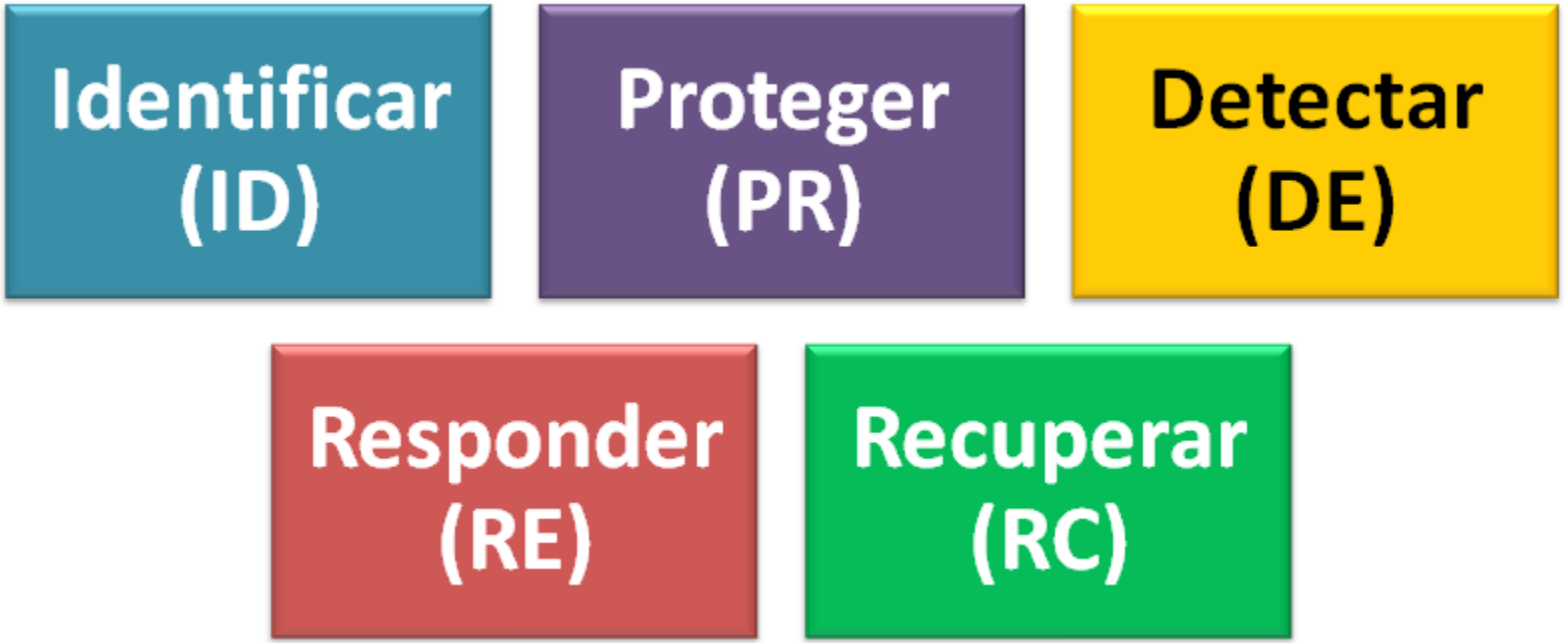


Atividades e Referências Informativas, organizadas de acordo a determinadas saídas.

Possibilita a comunicação dos riscos de cibersegurança na organização.

Descreve como os riscos de cibersegurança são priorizados pela organização.

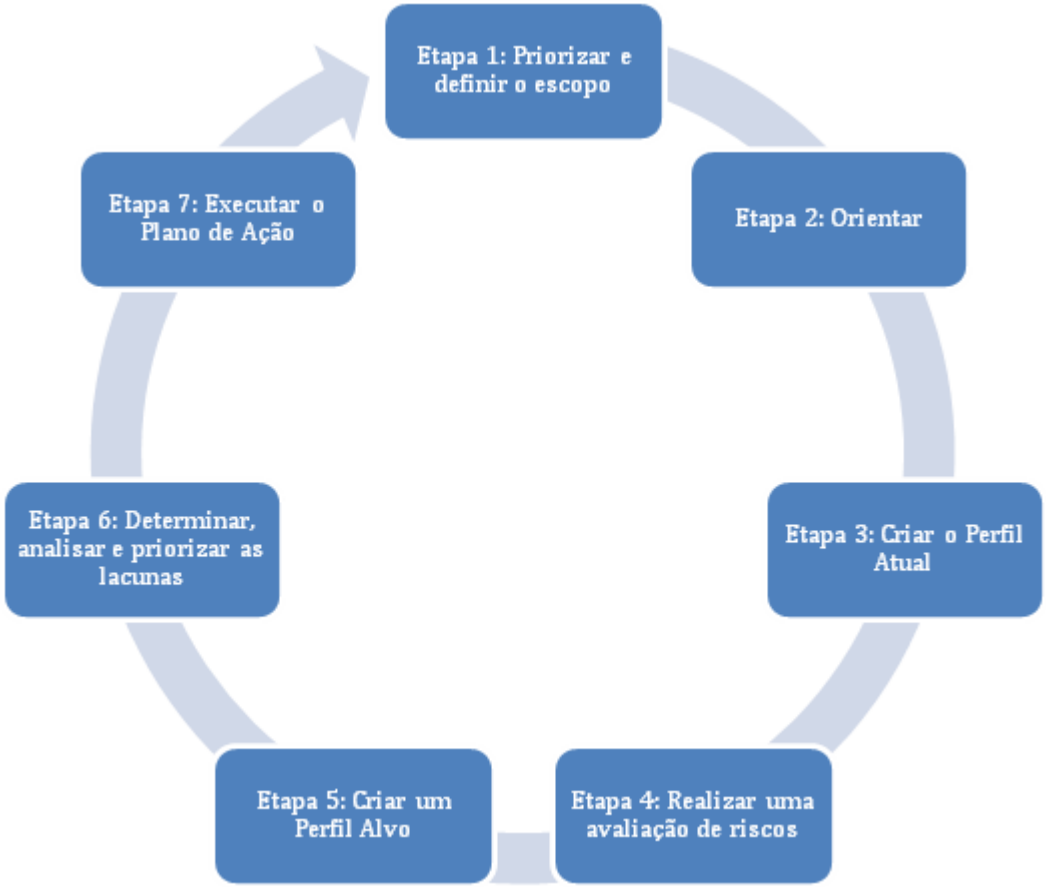
Núcleo do Framework



Amostra do Framework ABRATE

FUNÇÃO	CATEGORIA	SUBCATEGORIA	PRIORIDADE
PROTEGER (PR)	**Controle de acesso (PR.AC)**: O acesso a ativos e recursos associados é limitado a usuários, processos ou dispositivos autorizados e a atividades e transações autorizadas.	PR.AC-1: Identidades e credenciais são gerenciadas para dispositivos e usuários autorizados	Prioritário
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	Prioritário
		PR.AC-4: As permissões de acesso são gerenciadas, incorporando os princípios de menor privilégio e segregação de funções	Recomendável

Metodologia de Implementação



Modelo de Maturidade C2M2

Cybersecurity Capability Maturity Model

- Permite comparação e auxilia na definição de objetivos.
- Modelo de Maturidade desenvolvido pelo DOE.
- Possui 10 Domínios (assuntos ou áreas de conhecimento em Segurança Cibernética).
- Cada Domínio possui Objetivos (Macro Atividades relacionadas ao Domínio).
- Cada Objetivo possui práticas que devem ser cumpridas para avanço de um nível de maturidade para outro.

Domínios C2M2

ACM	• Ativos, Mudanças e Gerenciamento de Configurações
CPM	• Gestão do Programa de Segurança Cibernética
EDM	• Gerenciamento de Cadeia de Suprimentos e Dependências Externas
IAM	• Gerenciamento de Identidade e Acesso
IR	• Resposta a Eventos e Incidentes, Continuidade das Operações
ISC	• Compartilhamento de Informações e Comunicações
RM	• Gerenciamento de Riscos
SA	• Consciência Situacional
TVM	• Gestão de Ameaças e Vulnerabilidades
WM	• Gerenciamento da Força de Trabalho

Amostra de Objetivos e Práticas de um Domínio

ACM-1: Gerenciar inventário de ativos

ACM-2: Gerenciar configuração de ativos

a. As baselines de configuração são estabelecidas, pelo menos de maneira ad hoc, para os ativos inventariados aonde é desejável garantir que vários sejam configurados de forma semelhante.
c. O design de baselines de configuração inclui objetivos de segurança cibernética.
e. As baselines de configuração são revisadas e atualizadas em uma frequência definida organizacionalmente.

ACM-3: Gerenciar mudança de ativos

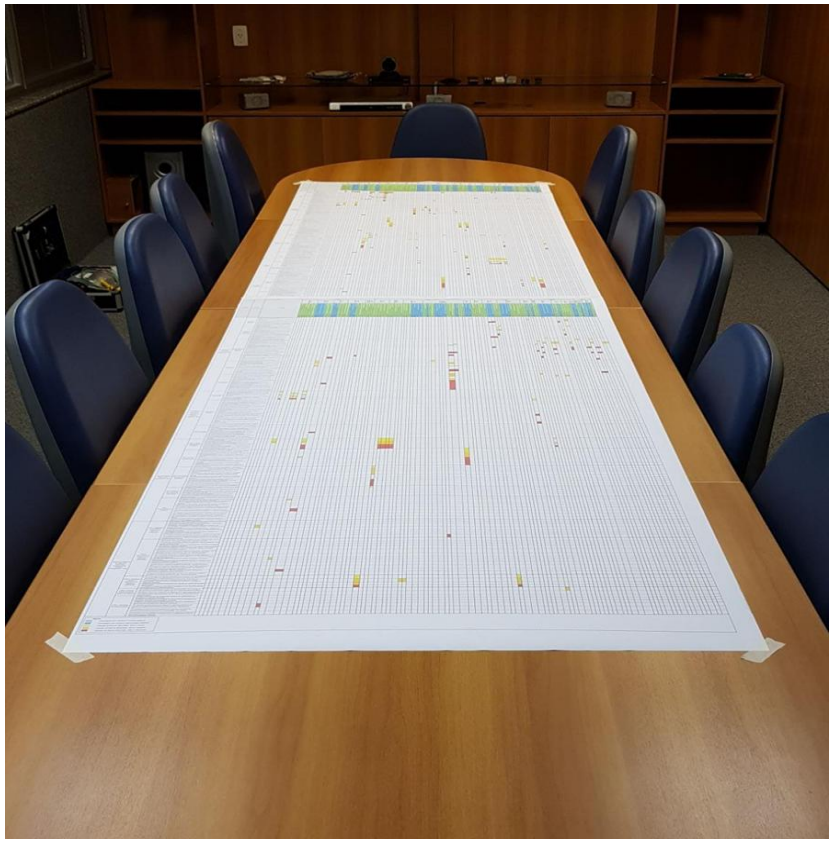
ACM-4: Atividades de gestão

Níveis de Maturidade C2M2

- Progressão:
  - Não Realizado (MIL0)
  - Ad-hoc (MIL1)
  - Práticas Documentadas (MIL2)
  - Políticas (MIL3)

Mapeamento ao C2M2

- Cada subcategoria do Framework possui uma série de práticas do C2M2.
- Práticas adicionais criadas pela ABRATE para complementar o C2M2.
- Definição do nível mínimo recomendável pela ABRATE de implantação.



Amostra do Mapeamento do Framework ao C2M2

MODELO DE MATURIDADE C2M2				IDENTIFICAR (ID)													
				GOVERNANÇA (ID.GV)				AVALIAÇÃO DE RISCO (ID.RA)						ESTRATÉGIA DE GERENCIAMENTO DE RISCO (ID.RM)			
DOMÍNIO	OBJETIVOS	PRÁTICAS		Política de segurança da informação da organização é estabelecida	Os papéis e responsabilidades de segurança da informação são coordenados e alinhados com funções internas e parceiros externos	Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo as obrigações de privacidade e das liberdades cívicas, são compreendidos e geridos	Processos de governança e gerenciamento de riscos tratam dos riscos de segurança cibernética	As vulnerabilidades dos ativos são identificadas e documentadas	Informações de ameaças e vulnerabilidades são recebidas de fóruns e fontes de compartilhamento de informações	Ameaças internas e externas são identificadas e documentadas	Os potenciais impactos ao negócio e as probabilidades são identificados	Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	As respostas ao risco são identificadas e priorizadas	Processos de gestão de riscos são estabelecidos, gerenciados e acordados pelas partes interessadas da	A tolerância ao risco organizacional é determinada e aprovada	A determinação da tolerância ao risco pela organização é subsidiada pelo seu papel na infraestrutura crítica e análise de risco específica do setor
				ID.GV-1	ID.GV-2	ID.GV-3	ID.GV-4	ID.RA-1	ID.RA-2	ID.RA-3	ID.RA-4	ID.RA-5	ID.RA-6	ID.RM-1	ID.RM-2	ID.RM-3
Gerenciamento de Risco (Risk Management - RM)	RM-2: Gerenciar o risco de segurança cibernética	a	Os riscos de segurança cibernética são identificados, pelo menos de forma *ad hoc*.				1						1*	1		
		b	Os riscos identificados são mitigados, aceitos, tolerados ou transferidos, pelo menos de maneira *ad hoc*.				1						1*	1		
		c	Avaliações de risco são realizadas para identificar riscos de acordo com a estratégia de gerenciamento de riscos.											2		
		d	Riscos identificados são documentados.											2		
		e	Os riscos identificados são analisados para priorizar as atividades de resposta de acordo com a estratégia de gerenciamento de riscos.										2	2		
		f	Os riscos identificados são monitorados de acordo com a estratégia de gerenciamento de risco.													
		g	A análise de risco é subsidiada pela arquitetura de rede (TI e / ou TO).											2		
		h	O Programa de Gerenciamento de Riscos define e opera políticas e procedimentos de gerenciamento de riscos que implementam a estratégia de gerenciamento de riscos.				3							3		
		i	Uma arquitetura atual de segurança cibernética é usada para informar a análise de risco.													
		j	Um registro de riscos (um repositório estruturado de riscos identificados) é usado para suportar atividades de gerenciamento de riscos.					3		3		3	3	3		

Exemplo de Práticas C2M2 mapeadas para a subcategoria ID-AM3

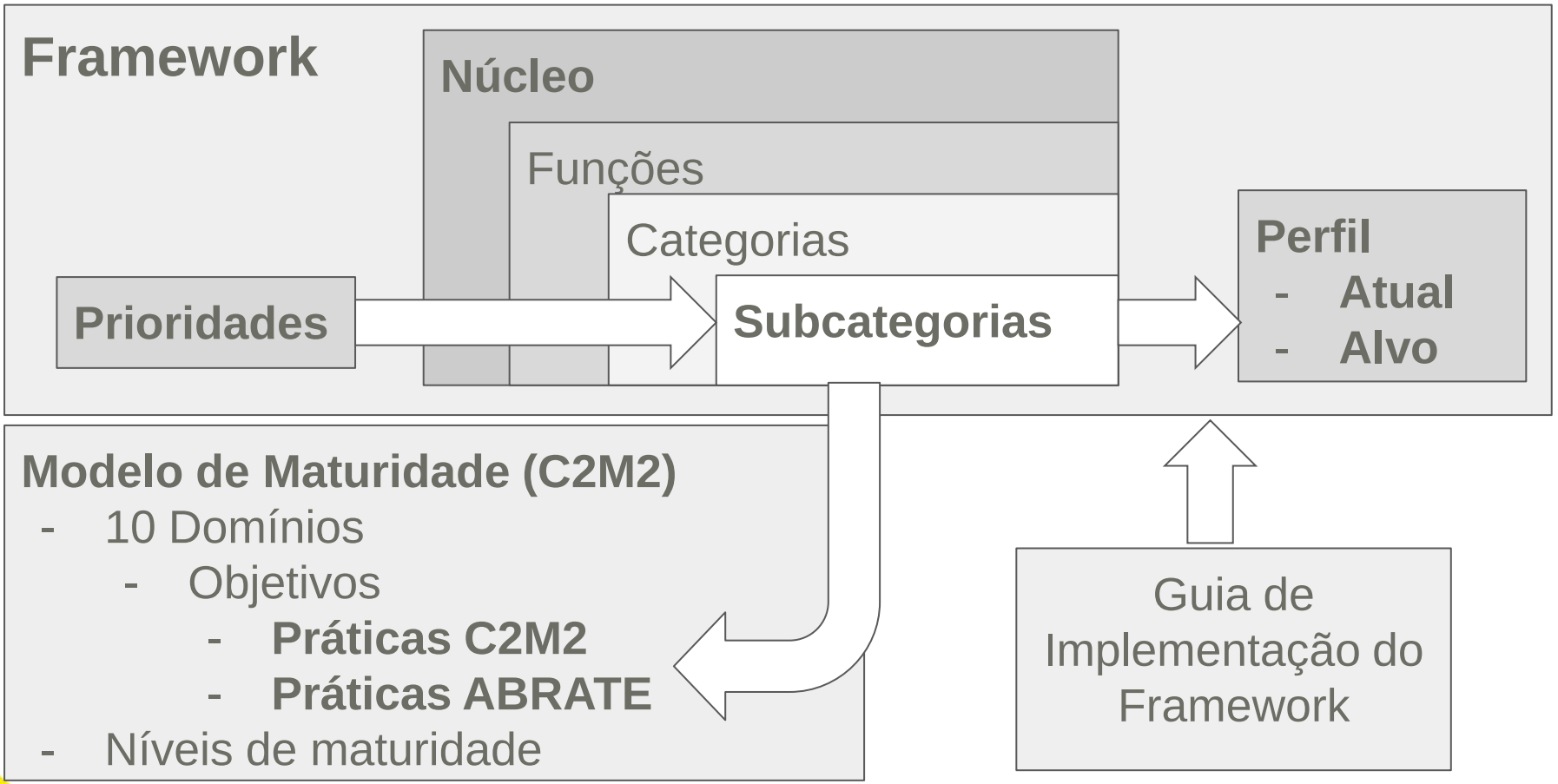
IDENTIFICAR (ID)

Gerenciamento de Ativos (AM)

ID.AM-3: Comunicação organizacional e fluxos de dados são mapeados

- MIL 1 - ABT-1a: Existe um documento descrevendo a filosofia de fluxo de dados na arquitetura de rede, pelo menos de maneira ad-hoc.
- MIL 2 - ABT-1b: Efetuar análise de risco com base no fluxo de dados, repositórios de dados, infraestrutura e conectividade.
- MIL 2 - RM-2g: A análise de risco é subsidiada pela arquitetura de rede (TI e/ou TO).
- MIL 3 - ACM-1e: Existe um inventário para todos os ativos conectados de TI e TO relacionados à entrega da função.

Overview


Framework
Núcleo
Funções
Categorias
Prioridades
Subcategorias
Perfil
- Atual
- Alvo
Modelo de Maturidade (C2M2)
- 10 Domínios
- Objetivos
- Práticas C2M2
- Práticas ABRATE
- Níveis de maturidade
Guia de Implementação do Framework

Conclusões

- Criado um Framework baseado no NIST/DOE para aplicação pelas empresas associadas à ABRATE
- O nível mínimo de implementação recomendado pela ABRATE pode ser aplicado por todas as empresas, com baixa oneração
- O Framework é aplicável a outras empresas do setor elétrico
- Há potencial para evoluir após experiências de sua implementação

Trabalhos Futuros

- Criação de um kit de ferramentas para auxiliar na avaliação/implementação.
- Estabelecer um processo de revisão permanente dos documentos.
- Treinamento para as empresas associadas.
- Apresentar o Framework ABRATE para ONS e outras Associações.