SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

PREFÁCIO

A Associação Brasileira das Empresas de Transmissão de Energia Elétrica (ABRATE) criou uma Força Tarefa de Segurança Cibernética, composta por representantes de empresas associadas, com o objetivo de criar um *framework* de segurança cibernética com foco em redes operacionais. Esse trabalho objetiva a definição de práticas de segurança cibernética em instalações de transmissão de energia elétrica, para os sistemas de telecomunicações, sistemas SCADA e demais recursos relacionados às redes de automação.

Como referência principal para elaboração do presente documento foi utilizado o *"Framework for Improving Critical Infrastructure Cybersecurity"*, do *National Institute of Standards and Technology* (NIST), o qual recomenda processos de gerenciamento de riscos que permitem às organizações informar e priorizar decisões relacionadas à segurança cibernética com base nas necessidades do negócio, sem requisitos regulamentares adicionais.

Para a elaboração deste framework, que servirá como arcabouço mínimo para elevar a segurança cibernética das instalações de missão crítica, foi adotado como premissa o atual modelo do setor elétrico brasileiro, no qual ocorre o compartilhamento de instalações entre diversos agentes e um considerável fluxo de dados entre redes diversas. Outro aspecto considerado foi a percepção de uma ausência de normas e procedimentos regulatórios que proporcionasse a padronização de requisitos relacionados à Segurança Cibernética de instalações críticas, tornando-as vulneráveis e podendo comprometer a disponibilidade do Sistema Interligado Nacional.

1 INTRODUÇÃO

O Framework foi construído considerando o ambiente de riscos do setor elétrico. Buscando a mitigação desses riscos, ferramentas e processos de gerenciamento de segurança cibernética podem ser utilizados pelas organizações para apoiar a implantação das melhores práticas aqui descritas.

O Framework foi projetado para auxiliar as organizações do setor elétrico a:

- Identificar o nível de segurança cibernética atual;
- Identificar o nível de segurança cibernética desejado;
- Identificar lacunas existentes nos programas de gerenciamento de risco em segurança cibernética, orientando e identificando áreas onde as práticas podem ser melhoradas;
- Identificar prioridades para implementação das práticas relativas aos níveis de maturidade
- Identificar ferramentas que possam apoiar a implantação do Framework;
- Demonstrar e comunicar de forma eficaz a abordagem de gerenciamento de riscos e uso do Framework para as partes interessadas, internas e externas.

2 PREPARAÇÃO PARA A IMPLANTAÇÃO DO FRAMEWORK

Esta seção ajuda na preparação para a implantação do Framework, apresentando a terminologia, os conceitos-chave e os principais benefícios do Framework. Consulte os glossários no Framework original do NIST e o Cybersecurity Capability Maturity Model (DOE - Department of Energy) para definições completas dos termos adicionais usados ao longo deste documento.

2.1 GUIA DE TERMINOLOGIA DO FRAMEWORK

Os três principais componentes do Framework são o Núcleo, os Níveis de Prioridade (definidos pela ABRATE) e os Perfis. Esses termos são frequentemente utilizados neste documento de orientação para implantação do Framework e definidos abaixo:

O Núcleo compreende três elementos: Funções, Categorias e Subcategorias. As funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento de segurança cibernética de uma organização. Existem cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar. Cada função é dividida em categorias e subcategorias. As categorias são objetivos de

segurança cibernética que estão ligados a atividades específicas. As subcategorias são os produtos específicos de atividades técnicas e/ou de gerenciamento, que garantem o sucesso de cada categoria. Os componentes do Núcleo do Framework estão listados resumidamente (Funções e Categorias) na Tabela 1.

Os Níveis de Prioridade orientam quanto às subcategorias que representam maior relevância para o gerenciamento de riscos em segurança cibernética. São definidos dois níveis: Prioritário e Recomendável.

Uma tabela completa com todos os componentes do Núcleo do Framework é apresentada no Apêndice A. Nesta tabela, o Nível de Prioridade das subcategorias com nível “Prioritário” estão marcadas em **negrito**, sendo o Nível de Prioridade das demais “Recomendável”

Função	Categoria
IDENTIFICAR (ID)	Gestão de Ativos (ID.AM): Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos comerciais são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos de negócios e a estratégia de risco da organização.
	Ambiente de Negócios (ID.BE): A missão, os objetivos, as partes interessadas e as atividades da organização são compreendidas e priorizadas; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.
	Governança (ID.GV): As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulamentares, legais, de risco, ambientais e operacionais da organização são compreendidos e informam o gerenciamento do risco de segurança cibernética.
	Avaliação de Risco (ID.RA): A organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem u reputação), ativos organizacionais e indivíduos.
	Estratégia de Gerenciamento de Risco (ID.RM): As prioridades, restrições, tolerâncias de risco e premissas da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.
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.
	Conscientização e Treinamento (PR.AT): O pessoal e os parceiros da organização recebem educação sobre conscientização sobre segurança cibernética e são adequadamente treinados para desempenhar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com políticas, procedimentos e acordos relacionados.

	Segurança de dados (PR.DS): 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 das informações.
	Processos e Procedimentos de Proteção da Informação (PR.IP): As políticas de segurança (que tratam de propósito, escopo, funções, responsabilidades, comprometimento de gerenciamento e coordenação entre entidades organizacionais), processos e procedimentos são mantidas e usadas para gerenciar a proteção de ativos e sistemas de informação.
	Manutenção (PR.MA): Manutenção e reparos de controles industriais e componentes do sistema de informação são realizados de forma consistente com políticas e procedimentos.
	Tecnologia de proteção (PR.PT): Soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência de sistemas e ativos, consistentes com políticas, procedimentos e acordos relacionados.
DETECTAR (DE)	Anomalias e Eventos (DE.AE): A atividade anômala é detectada em tempo hábil e o impacto potencial dos eventos é compreendido.
	Monitoramento Contínuo de Segurança (DE.CM): Os sistemas de informação e os ativos são monitorados em intervalos discretos para identificar eventos de segurança cibernética e verificar a eficácia de medidas de proteção.
	Processos de Detecção (DE.DP): Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização adequada e oportuna de eventos anômalos.
RESPONDER (RS)	Planejamento de Respostas (RS.RP): Processos e procedimentos de resposta são executados e mantidos, para garantir a resposta oportuna aos eventos de segurança cibernética detectados.
	Comunicações (RS.CO): As atividades de resposta são coordenadas com as partes interessadas internas e externas, conforme apropriado.
	Análise (RS.AN): A análise é conduzida para assegurar uma resposta adequada e apoiar as atividades de recuperação.
	Mitigação (RS.MI): As atividades são realizadas para impedir a expansão de um evento, mitigar seus efeitos e erradicar o incidente.
	Melhorias (RS.IM): As atividades de resposta organizacional são aprimoradas pela incorporação de lições aprendidas de atividades de detecção / resposta atuais e anteriores.
RECUPERAR (RC)	Planejamento de Recuperação (RC.RP): Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração em tempo hábil de sistemas ou ativos afetados por eventos de segurança cibernética.
	Melhorias (RC.IM): O planejamento e os processos de recuperação são aprimorados pela incorporação de lições aprendidas em atividades futuras.
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas.

Tabela 1 – Funções e Categorias do Núcleo do Framework

Os Perfis alinham os principais elementos do Framework aos requisitos de negócios, tolerância ao risco e recursos organizacionais. O Perfil pode ser usado para identificar oportunidades para melhorar a posição de segurança cibernética, comparando um Perfil Atual com um Perfil Alvo. Os Perfis fornecem um roteiro para reduzir o risco em segurança cibernética de acordo com as práticas do negócio e boas práticas de mercado.

Este documento também utiliza frequentemente o termo organização, que descreve uma entidade operacional de qualquer porte que usa o mesmo programa de gerenciamento de risco em segurança cibernética dentro de seus diferentes componentes e pode usar individualmente o Framework. Isso pode descrever uma corporação ou uma unidade de negócios ou processo dentro de uma corporação de várias unidades. Como cada empresa pode desenvolver e implantar seus programas de gerenciamento de risco em diferentes níveis, essa orientação é projetada para qualquer organização - seja a organização toda a empresa ou uma unidade de negócios ou processo dentro da empresa.

2.2 ORIENTAÇÕES SOBRE OS CONCEITOS DO FRAMEWORK

Este documento oferece orientações para todas as organizações, independentemente da maturidade de seus programas de segurança cibernética e de gerenciamento de riscos.

Para organizações que não possuem um programa de gerenciamento de riscos em segurança cibernética, este guia ajudará a implantar o Framework diretamente ou a selecionar uma abordagem alternativa (como conjuntos de padrões ou ferramentas de segurança e gerenciamento de riscos amplamente utilizados) que implantará o Framework indiretamente, através de seu uso.

Para organizações que possuem um programa de gerenciamento de riscos em segurança cibernética, este documento ajudará a revisar o programa existente, identificando quaisquer falhas de segurança ou gerenciamento de riscos e alinhando-o com os principais elementos do Framework. Alinhar abordagens ao Framework pode ajudar a organização na apresentação de sua implantação e na comunicação sobre seu perfil de riscos de segurança cibernética com as partes interessadas.

Para usar o Framework, uma organização não precisa relacionar diretamente todos os elementos de seu programa de segurança cibernética aos elementos do Framework. Entretanto, organizações que desejam demonstrar seu alinhamento com o Framework são recomendadas a revisar e documentar o alinhamento de seus programas e práticas.

2.3 PROCESSO E BENEFÍCIOS DA IMPLANTAÇÃO DO FRAMEWORK

O Framework e estas orientações são projetadas para serem flexíveis o suficiente para serem usadas tanto por organizações do setor elétrico com programas maduros de segurança cibernética e de gerenciamento de riscos, como por aqueles com programas menos desenvolvidos. Cada organização escolherá se, como e onde usará o Framework com base em seu próprio ambiente operacional. A escolha de implantar o Framework não implica que uma abordagem existente de segurança cibernética e gerenciamento de riscos seja ineficaz ou precise ser substituída. Pelo contrário, isso significa que a organização deseja aproveitar os benefícios que o Framework oferece.

A implantação do Framework fornece um mecanismo que permite às organizações:

- Identificar sua atual posição em segurança cibernética em termos de funções, objetivos de categoria e resultados de subcategoria, para as partes interessadas;
- Descrever o Perfil Atual e Perfil Desejado para seus programas de segurança cibernética;
- Avaliar o progresso em direção ao Perfil Desejado;
- Identificar e priorizar oportunidades de melhoria dentro do contexto de um processo contínuo e repetitivo;
- Comunicar o Perfil Atual, o Perfil Desejado e outras informações de gerenciamento de risco em segurança cibernética às partes interessadas.

A implantação do Framework pode ajudar as organizações a fortalecer sua abordagem existente em gerenciamento de riscos de segurança cibernética e comunicar mais facilmente a utilização de práticas específicas de segurança cibernética a partes interessadas. Organizações com programas de gerenciamento de riscos de segurança cibernética menos desenvolvidos podem usar o Framework para definir e estabelecer um programa para tratar os riscos de segurança cibernética, relativos aos objetivos de negócios e da infraestrutura crítica da organização.

A abordagem de implantação detalhada na Seção 4 orienta as organizações a mapear suas abordagens existentes de gerenciamento de riscos em segurança cibernética (por exemplo, padrões, ferramentas, métodos e diretrizes) ao Núcleo do Framework. O mapeamento pode:

- Identificar as lacunas entre os resultados alcançados pela abordagem da organização e os resultados definidos no Núcleo do Framework e no Perfil Desejado. A organização pode tomar medidas para corrigir essas lacunas ou determinar que essas não sejam significativas ou relevantes para o gerenciamento de seus riscos de segurança

cibernética. No entanto, a organização pode se beneficiar da identificação e documentação dessas lacunas para facilitar a comunicação sobre o uso que a organização faz do Framework.

- Identificar áreas em que a abordagem da organização é mais abrangente do que o Núcleo do Framework. Devido a riscos específicos de infraestrutura organizacional ou crítica, uma organização pode implantar abordagens de segurança cibernética que alcancem resultados que vão além dos resultados descritos pelas Categorias Principais e Subcategorias do Framework. Essas organizações também podem se beneficiar da identificação e documentação dessas lacunas para facilitar a comunicação de riscos com partes interessadas. Quando apropriado, as organizações do setor elétrico devem considerar o compartilhamento de sua abordagem de gerenciamento de risco com a ABRATE para ajudar a fortalecer e expandir o Framework.

Idealmente, o Framework deve ser incorporado como parte de um programa de melhoria contínua do processo de gerenciamento de riscos em segurança cibernética.

3 RECURSOS PARA A IMPLANTAÇÃO DO FRAMEWORK NO SETOR

Esta seção apresenta uma visão geral de algumas das ferramentas e processos de segurança cibernética, atualmente em uso pelo setor elétrico, que podem suportar a implantação do Framework.

3.1 EXEMPLOS DE ABORDAGEM NO GERENCIAMENTO DE RISCOS DE SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO

Várias ferramentas, processos, padrões e diretrizes de gerenciamento de riscos de segurança cibernética já amplamente utilizados pelas organizações do setor elétrico podem se alinhar com as abordagens de segurança e gerenciamento de riscos do Framework e ajudar a demonstrar como a organização já está aplicando seus conceitos. Embora este documento de orientação forneça apenas o mapeamento de uma ferramenta - o C2M2 (Cybersecurity Capability Maturity Model) - para o Framework, outras abordagens podem dar suporte a uma organização no mapeamento de seu programa para o Framework. Um conjunto de exemplos de abordagens amplamente disponíveis, utilizadas no setor elétrico, está apresentado na Tabela 2. Outras ferramentas e processos, disponíveis ou em desenvolvimento, também podem fornecer recursos semelhantes no gerenciamento de riscos de segurança cibernética.

Nome	Resumo	Informações Adicionais
Cybersecurity Capability Maturity Model (C2M2), em ambas as versões específicas para o Setor Elétrico e Óleo e Gás Natural	Usado para avaliar a capacidade da segurança cibernética de uma organização e priorizar suas ações e investimentos para melhorar sua segurança cibernética	http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2
Cyber Resilience Review (CRR)	Avalia as práticas de resiliência operacional e segurança cibernética de uma organização em dez diferentes domínios	https://www.us-cert.gov/ccubedvp/self-service-crr
Cyber Security Evaluation Tool (CSET)	Orienta os usuários por meio de um processo passo a passo para avaliar seu sistema de controle e práticas de segurança de rede em relação a padrões reconhecidos na indústria	http://ics-cert.us-cert.gov/Assessments
Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline	Permite que as organizações apliquem processos de gerenciamento de riscos eficazes e eficientes adaptando-os para atender aos seus requisitos organizacionais	http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012
Critical Infrastructure Protection (CIP) Standards	Os Padrões CIP da NERC (North American Electric Reliability Corporation) fornecem um conjunto de requisitos de segurança cibernética para ajudar a proteger os ativos do sistema de energia que operam e mantém a rede elétrica	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
ISA/IEC62443	Padrões multi-setoriais que listam métodos e técnicas de proteção de segurança cibernética para ambientes SCADA. É uma derivação dos padrões ISO 27000 com foco em Sistemas de Controle Industriais	https://isasecure.org

Tabela 2 – Exemplo de Abordagens de Gerenciamento de Risco de Segurança Cibernética

3.2 MAPEANDO PARA O FRAMEWORK

A Seção 5 detalha uma abordagem de implantação do Framework usando o C2M2, e um mapeamento do C2M2 para o Framework é fornecido no Apêndice A. Fornecedores e

desenvolvedores de padrões também podem ter desenvolvido separadamente mapeamentos de outras ferramentas e processos para o Framework. As organizações podem usar esses mapeamentos juntamente com esta orientação para suportar o uso do Framework.

As organizações podem mapear sua abordagem atual de segurança cibernética aos elementos do Framework, usando mapeamentos específicos de ferramentas como guia, sempre que possível. O mapeamento não apenas apoia a capacidade de uma organização de identificar possíveis lacunas que necessitem ser abordadas, mas também pode destacar onde o Framework não descreve adequadamente a abordagem de segurança cibernética da organização. Um mapeamento claro fornece uma tradução entre as práticas atuais da organização e do Framework, apoiando a comunicação com partes interessadas. Consulte a Etapa 3 na Seção 4 para obter orientação sobre o uso de mapeamentos com o Framework.

4 ABORDAGEM PARA A IMPLANTAÇÃO DO FRAMEWORK

Esta seção apresenta uma abordagem padrão para usar o Framework (Figura 1) que está alinhado com o processo de sete etapas descritas abaixo:

- Etapa 1: Priorizar e Definir o Escopo
- Etapa 2: Orientar
- Etapa 3: Criar um Perfil Atual
- Etapa 4: Realizar uma avaliação de riscos
- Etapa 5: Criar um Perfil Alvo
- Etapa 6: Determinar, Analisar e Priorizar Lacunas
- Etapa 7: Executar o Plano de Ação

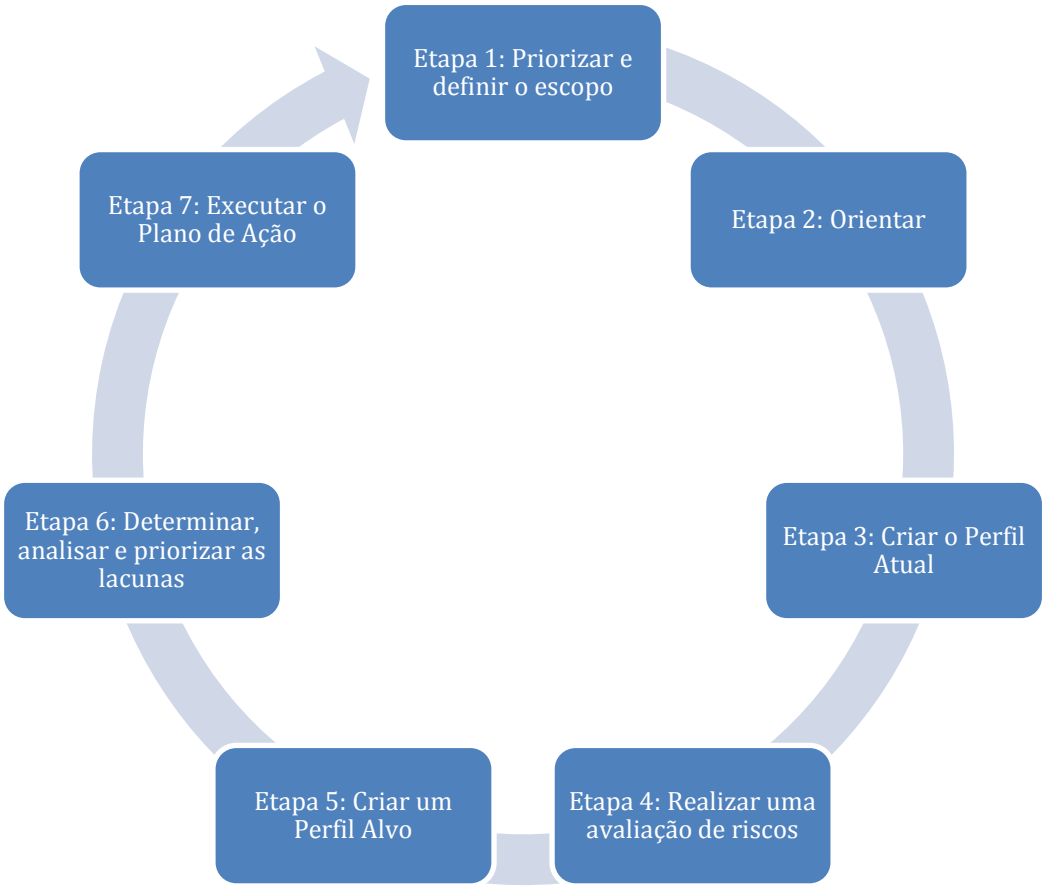

Figura 1 – Abordagem para Implantação do Framework

Essa abordagem pode ser utilizada em conjunto com qualquer padrão de segurança cibernética, ferramenta específica do setor elétrico ou ferramenta comercial para gerenciar o risco de segurança cibernética - como os descritos na Seção 3 deste documento - para facilitar a implantação do Framework. (Como exemplo, a Seção 5 deste documento explica como a implantação do C2M2 se enquadra nessa abordagem).

Cada etapa é apresentada por uma tabela que descreve suas entradas, atividades e saídas. Explicações adicionais são fornecidas abaixo de cada tabela. Um resumo das entradas, atividades e saídas para cada etapa está incluído no Apêndice C.

Muitas organizações do setor elétrico já possuem programas abrangentes de gerenciamento de risco que estabelecem o contexto para decisões baseadas em risco, permitindo-lhes avaliar, abordar e monitorar o risco de forma contínua. Muitas também usam comunicações eficazes e um ciclo de feedback interativo para melhoria contínua. Para essas organizações as atividades descritas nestas sete etapas provavelmente já foram executadas e a implantação do Framework é, em grande parte, uma questão de descrever e alinhar ou “traduzir” elementos de sua abordagem atual para os elementos do Núcleo do Framework.

Etapa 1: Priorizar e Definir o Escopo

Entradas	Atividades	Saídas
• Estratégia de gerenciamento de risco • Objetivos organizacionais e prioridades • Informações sobre ameaças	• Determinar onde será aplicado o Framework para avaliar e potencialmente guiar a melhoria dos recursos de segurança cibernética da organização	• Escopo de uso do framework

Um processo de gerenciamento de riscos geralmente inclui uma estratégia que aborda como identificar, avaliar, responder e monitorar o risco. Se a organização é uma unidade em uma empresa maior, ela pode estar usando uma estratégia em nível corporativo em vez de uma estratégia exclusiva em nível organizacional. Independentemente disso, a estratégia aplicável descreve de forma explícita e transparente os riscos organizacionais identificados que a organização utiliza rotineiramente para informar as decisões operacionais e de investimento. Essa estratégia pode ser informada por objetivos e prioridades de proteção de infraestrutura, crítica de todo o setor, que geralmente são preocupações compartilhadas entre os setores público e privado.

Nesta etapa, a organização decide como e onde deseja usar o Framework (escopo de uso), seja em um subconjunto de suas operações, em vários subconjuntos de suas operações ou para toda a organização. Essa decisão deve se basear em considerações de gerenciamento de riscos, objetivos e prioridades da infraestrutura organizacional e crítica, disponibilidade de recursos e outros fatores internos e externos.

Uma organização que esteja usando o Framework pela primeira vez pode querer aplicá-lo a um pequeno subconjunto de operações para ganhar familiaridade e experiência com ele. Após essa atividade, a organização pode considerar a aplicação do Framework a um subconjunto mais amplo de operações ou a partes adicionais da organização, conforme apropriado.

Etapa 2: Orientar

Entradas	Atividades	Saídas
• Escopo de uso do framework • Estratégia de gerenciamento de risco	• Identificar os sistemas e ativos dentro do escopo (por exemplo, pessoas, informações, tecnologia e instalações) e as referências normativas e informativas apropriadas (por exemplo, padrões, ferramentas, métodos e diretrizes de segurança cibernética e de riscos)	• Sistemas e ativos dentro do escopo • Requisitos de escopo (ou seja, regulatório, empresarial, organizacional) • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • Método de avaliação

A organização identifica os sistemas, ativos, requisitos e métodos de gerenciamento de risco de segurança cibernética que estão no escopo. Isso inclui padrões e práticas que a organização já usa e pode incluir padrões e práticas adicionais que a organização acredita que ajudariam a alcançar seus objetivos de gerenciamento de riscos de segurança cibernética relativos a sua infraestrutura crítica e seu negócio. O programa de gerenciamento de risco da organização pode já ter identificado e documentado grande parte dessas informações ou pode ajudar a identificá-las. Uma regra geral é concentrar inicialmente em sistemas e ativos críticos e, então, expandir o foco para sistemas e ativos menos críticos, conforme os recursos permitirem.

A organização também deve escolher o método de avaliação que utilizará para identificar sua situação de segurança cibernética para criar um perfil atual. Para isto, o método pode incluir autoavaliações, através das quais a organização pode alavancar seus próprios recursos e conhecimentos, ou outros métodos, em que a avaliação é realizada por terceiros.

Etapa 3: Criar um Perfil Atual

Entradas	Atividades	Saídas
• Sistemas e ativos dentro do escopo • Requisitos regulatórios de escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • Método de avaliação	• Identificar a situação de segurança cibernética e gerenciamento de riscos da Organização	• Perfil atual

A organização cria um Perfil Atual, mapeando suas práticas existentes em segurança

cibernética e gerenciamento de riscos para descrições específicas no documento do Framework. É importante entender que o propósito de identificar um Perfil Atual não é simplesmente criar um mapa entre práticas organizacionais e resultados de Categoria e Subcategoria, mas também entender como essas práticas atingem os resultados delineados pelo Framework.

Para identificar o Perfil Atual, a organização usa o método de avaliação determinado na Etapa 2 para mapear a situação de segurança cibernética existente, relacionando com os objetivos de Categoria e Subcategoria listados no Apêndice A do documento do Framework (chamado de Núcleo do Framework). As organizações já podem realizar essas avaliações como parte da avaliação de riscos ou ter processos definidos que possam ser aproveitados para identificar sua situação atual. Por exemplo, muitas organizações realizam avaliações regulares de seus programas de segurança cibernética por meio de auditorias internas ou atividades semelhantes. As saídas dessas atividades podem descrever quais práticas são executadas para sistemas e ativos dentro do escopo e podem ser usadas para essa etapa.

A Tabela 3 fornece um exemplo de como um mapeamento pode ser utilizado para criar um perfil atual para um resultado de subcategoria específico (PR.AC-3) para três organizações que usam três abordagens diferentes. Observe que os exemplos nessas tabelas pretendem ilustrar o conceito de mapeamento e provavelmente não refletirão situações específicas de qualquer organização. O nível de especificidade e granularidade necessário é de caráter individual para cada organização.

Organização 1

Abordagem de Controles Internos

Função	Categoria	Subcategoria	Perfil Atual
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	Acesso discado para manutenção de fornecedores é ativado conforme necessário e desativado quando a janela de manutenção é concluída
			Acesso remoto autorizado apenas por meio de serviço VPN criptografado
			Atividade de acesso remoto registrada e monitorada
			Acesso ao serviço VPN restrito a dispositivos aprovados pela organização
			Todas as tentativas de conexão não autorizadas à VPN são registradas

			Desativação imediata da conta VPN na rescisão do funcionário

Organização 2

Abordagem Baseada em Padrões

Função	Categoria	Subcategoria	Perfil Atual
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	NIST SP 800-53 Rev 4 AC-17
			NIST SP 800-53 Rev 4 AC-17 (1)
			NIST SP 800-53 Rev 4 AC-17 (2)
			NIST SP 800-53 Rev 4 AC-19
			NIST SP 800-53 Rev 4 AC-20
			NIST SP 800-53 Rev 4 AC-20 (1)

Organização 3

Abordagem de Exceção

Função	Categoria	Subcategoria	Perfil Atual
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	Não aplicável - Nenhum acesso remoto disponível para ativos em escopo e sistemas

Tabela 3 – Mapeando a Abordagem Organizacional ao Framework

Embora o Framework forneça ampla cobertura dos domínios de segurança cibernética e gerenciamento de riscos, ele pode não ser suficientemente abrangente e a organização pode ter implementado padrões, ferramentas, métodos e diretrizes que atingem resultados não definidos ou referenciados no Framework. O perfil atual deve identificar essas práticas também.

Etapa 4: Realizar uma avaliação de riscos

Entradas	Atividades	Saídas
• Escopo de uso do Framework • Estratégia de Gerenciamento de Risco • Abordagem de avaliação de risco definida pela organização • Requisitos regulamentares no escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo	• Realizar avaliação de risco para o escopo da organização	• Relatório de avaliação de risco

As organizações realizam avaliações para identificar e analisar riscos de segurança cibernética e determinar quais estão fora das tolerâncias atuais. Os resultados das atividades de avaliação de risco de segurança cibernética auxiliam a organização no desenvolvimento de seu Perfil Alvo, que ocorre na Etapa .

Etapa 5: Criar um Perfil Alvo

Entradas	Atividades	Saídas
• Perfil atual • Objetivos organizacionais • Estratégia de gerenciamento de riscos • Relatório de avaliação de riscos	• Identificar metas que mitigarão o risco de acordo com seus objetivos	• Perfil Alvo

Ao criar um Perfil Alvo, a organização deve considerar:

- Práticas atuais de gerenciamento de risco
- Ambiente de risco atual
- Requisitos legais e regulamentares
- Objetivos de negócios e missão
- Restrições organizacionais

O Perfil Alvo identifica os resultados desejados de Categoria e Subcategoria e os padrões, ferramentas, métodos e diretrizes que mitigarão os riscos de segurança cibernética, de acordo com

os objetivos organizacionais.

Conforme observado na Etapa 3, o Framework fornece ampla cobertura dos domínios de segurança cibernética e gerenciamento de riscos, mas pode não atender todas as demandas da organização, sendo necessário implantar padrões, ferramentas, métodos e diretrizes que atinjam resultados não definidos pelo Framework. O Perfil Alvo também deve identificar essas práticas.

A Tabela 4 fornece um exemplo de um Perfil Alvo para um resultado de Subcategoria específico (PR.AC-3) para três organizações que usam três abordagens diferentes. O texto em negrito e em itálico no Perfil Alvo destaca onde a organização identificou práticas adicionais que deseja usar para alcançar com êxito um resultado com base em seu ambiente de risco atual e objetivos de negócio. A Organização 1 determinou que suas práticas atuais de gerenciamento de acesso remoto não são adequadas para lidar com seu próprio ambiente de risco e identifica práticas adicionais necessárias. A organização 2 chega à mesma conclusão e identifica padrões adicionais que deseja implantar na organização dentro do escopo. A organização 3 possui um Perfil Alvo idêntico ao Perfil Atual para essa subcategoria. Esse será o caso quando os padrões, ferramentas, métodos e diretrizes atualmente implantados pela organização atendem aos requisitos de segurança cibernética e gerenciamento de riscos. No entanto, essa equidade entre Perfil Atual e Perfil Alvo pode ser apenas temporária, pois os requisitos de segurança e gerenciamento de riscos da organização podem evoluir com a mudança dos seus ambientes operacionais e de risco. Embora não esteja incluída em um exemplo, uma organização pode determinar que uma prática atual não é mais necessária ou inadequada e pode ser omitida do Perfil Alvo.

Ao desenvolver um Perfil Alvo, as organizações podem adotar uma abordagem ampla - considerando abordagens de gerenciamento de risco mais eficazes e eficientes em todo o escopo da organização - em vez de examinar categorias e subcategorias individuais.

Usando sua coleção de padrões, ferramentas, métodos e diretrizes de segurança e gerenciamento de riscos, a organização documenta esses resultados desejados no Perfil Alvo.

Organização 1

Abordagem de Controles Internos

Função	Categoria	Subcategoria	Perfil Atual	Perfil Alvo
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	O acesso discado para manutenção de fornecedores é ativado conforme necessário e desativado quando a janela de manutenção é concluída	O acesso discado para manutenção de fornecedores é ativado conforme necessário e desativado quando a janela de manutenção é concluída
			Acesso remoto autorizado apenas por meio de serviço VPN criptografado	Acesso remoto autorizado apenas por meio de serviço VPN criptografado
			Atividade de acesso remoto registrada e monitorada	Atividade de acesso remoto registrada e monitorada
			Acesso ao serviço VPN restrito a dispositivos aprovados pela organização	Acesso ao serviço VPN restrito a dispositivos aprovados pela organização
			Todas as tentativas de conexão não autorizadas à VPN são registradas	Todas as tentativas de conexão não autorizadas à VPN são registradas
			Desativação imediata da conta VPN na rescisão do funcionário	Desativação imediata da conta VPN na rescisão do funcionário
				Requerida assinatura do Supervisor antes da emissão da conta de VPN
				Revisão Bianual de autorização da lista de contas VPN

Organização 2

Abordagem Baseada em Padrões

Função	Categoria	Subcategoria	Perfil Atual	Perfil Alvo
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	NIST SP 800-53 Rev 4 AC-17	NIST SP 800-53 Rev 4 AC-17
			NIST SP 800-53 Rev 4 AC-17 (1)	NIST SP 800-53 Rev 4 AC-17 (1)
			NIST SP 800-53 Rev 4 AC-17 (2)	NIST SP 800-53 Rev 4 AC-17 (2)
				NIST SP 800-53 Rev 4 AC-17 (3)
				NIST SP 800-53 Rev 4 AC-17 (4)
			NIST SP 800-53 Rev 4 AC-19	NIST SP 800-53 Rev 4 AC-19
				NIST SP 800-53 Rev 4 AC-19 (5)
			NIST SP 800-53 Rev 4 AC-20	NIST SP 800-53 Rev 4 AC-20
			NIST SP 800-53 Rev 4 AC-20 (1)	NIST SP 800-53 Rev 4 AC-20 (1)
				NIST SP 800-53 Rev 4 AC-20 (2)

Organização 3

Abordagem de Exceção

Função	Categoria	Subcategoria	Perfil Atual	Perfil Alvo
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	Não aplicável - Nenhum acesso remoto disponível para ativos em escopo e sistemas	Não aplicável - Nenhum acesso remoto disponível para ativos em escopo e sistemas

Tabela 4 – Criando um Perfil Alvo

O texto em negrito realça as diferenças entre o Perfil Atual e Perfil Alvo.

Etapa 6: Determinar, Analisar e Priorizar Lacunas

Entradas	Atividades	Saídas
• Perfil Atual • Perfil Alvo • Objetivos Organizacionais • Impacto para Infraestrutura Crítica • Lacunas e Potenciais Consequências • Restrições Organizacionais • Estratégia de Gerenciamento de Risco • Relatórios de Avaliação de Risco	• Análisar as lacunas entre o Perfil Atual e o Perfil Alvo no contexto de organização • Avaliar potenciais consequências advindas das lacunas • Determinar quais lacunas precisam de atenção • Identificar ações para endereçar as lacunas • Realizar análise de custo-benefício • Priorizar ações (Custo-benefício e Consequências) • Planejar a implementação de ações	• Lacunas priorizadas e potenciais consequências • Plano de implementação priorizado

A organização avalia seu Perfil Atual em relação ao seu Perfil Alvo e identifica as lacunas. É importante incluir informações de todas as partes interessadas da organização para garantir que os objetivos de negócio sejam considerados no processo de priorização.

Existe uma lacuna quando há um resultado de Categoria ou Subcategoria no Perfil Alvo que atualmente não é alcançado pela abordagem de segurança e gerenciamento de risco existente da organização. O texto em negrito na Tabela 5 fornece alguns exemplos muito simples de como as organizações podem identificar lacunas.

Depois de identificar lacunas no perfil, a organização determina as possíveis consequências de não resolvê-las. Uma prioridade de mitigação deve então ser atribuída a todas as lacunas identificadas. A priorização deve incluir a consideração das práticas atuais de gerenciamento de risco, o ambiente atual de riscos, os requisitos legais e regulamentares, missão e objetivos do negócio, e quaisquer restrições organizacionais aplicáveis.

Uma vez que a cada lacuna é atribuída uma prioridade de mitigação, a organização identifica potenciais atividades de mitigação e realiza uma análise de custo-benefício sobre essas ações potenciais. A organização desenvolve um plano de ações de mitigação priorizadas - com base nos recursos disponíveis, nas necessidades do negócio e no ambiente de risco atual - para passar do Perfil Atual para o Perfil Alvo. Se a organização estiver no seu Perfil Alvo, ela procurará manter sua postura de segurança à medida em que o cenário de risco muda.

Organização 1

Abordagem de Controles Internos

Função	Categoria	Subcategoria	Perfil Atual	Alvo	Lacuna
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: O Acesso Remoto Gerenciado	O acesso discado para manutenção de fornecedores é ativado conforme necessário e desativado quando a janela de manutenção é concluída	O acesso discado para manutenção de fornecedores é ativado conforme necessário e desativado quando a janela de manutenção é concluída	
			Acesso remoto autorizado apenas por meio de serviço VPN criptografado	Acesso remoto autorizado apenas por meio de serviço VPN criptografado	
			Atividade de acesso remoto registrada e monitorada	Atividade de acesso remoto registrada e monitorada	
			Acesso ao serviço VPN restrito a dispositivos aprovados pela organização	Acesso ao serviço VPN restrito a dispositivos aprovados pela organização	
			Todas as tentativas de conexão não autorizadas à VPN são registradas	Todas as tentativas de conexão não autorizadas à VPN são registradas	
			Desativação imediata da conta VPN na rescisão do funcionário	Desativação imediata da conta VPN na rescisão do funcionário	
				Requerida assinatura do Supervisor antes da emissão da conta de VPN	**Requerida assinatura do Supervisor antes da emissão da conta de VPN**
				Revisão Bianual de autorização da lista de contas VPN	**Revisão Bianual de autorização da lista de contas VPN**

Organização 2

Abordagem Baseada em Padrões

			Atual	Alvo	Lacuna
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: O Acesso Remoto Gerenciado	NIST SP 800-53 Rev 4 AC-17	NIST SP 800-53 Rev 4 AC-17	
			NIST SP 800-53 Rev 4 AC-17 (1)	NIST SP 800-53 Rev 4 AC-17 (1)	
			NIST SP 800-53 Rev 4 AC-17 (2)	NIST SP 800-53 Rev 4 AC-17 (2)	
				NIST SP 800-53 Rev 4 AC-17 (3)	**NIST SP 800-53 Rev 4 AC-17 (3)**
				NIST SP 800-53 Rev 4 AC-17 (4)	**NIST SP 800-53 Rev 4 AC-17 (4)**
			NIST SP 800-53 Rev 4 AC-19	NIST SP 800-53 Rev 4 AC-19	
				NIST SP 800-53 Rev 4 AC-19 (5)	**NIST SP 800-53 Rev 4 AC-19 (5)**
			NIST SP 800-53 Rev 4 AC-20	NIST SP 800-53 Rev 4 AC-20	
			NIST SP 800-53 Rev 4 AC-20 (1)	NIST SP 800-53 Rev 4 AC-20 (1)	
				NIST SP 800-53 Rev 4 AC-20 (2)	**NIST SP 800-53 Rev 4 AC-20 (2)**

Organização 3

Abordagem de Exceção

Função	Categoria	Subcategoria	Perfil Atual	Perfil Alvo	Lacuna
PROTEGER (PR)	Controle de Acesso (PR.AC)	PR.AC-3: Acesso Remoto Gerenciado	Não aplicável - Nenhum acesso remoto disponível para ativos em escopo e sistemas	Não aplicável - Nenhum acesso remoto disponível para ativos em escopo e sistemas	Não há

Tabela 5 – Identificando lacunas de implementação

Etapa 7: Executar o Plano de Ação

Entradas	Atividades	Saídas
• Plano de implementação priorizado	• Implementar ações por prioridade • Acompanhar o progresso em relação ao plano • Monitorar e avaliar os principais riscos, indicadores de desempenho e métricas • Relatório de Progresso	• Dados de acompanhamento do plano • Novas medidas de segurança implementadas

A organização executa o plano de implementação e acompanha seu progresso ao longo do tempo, garantindo que as lacunas sejam fechadas e os riscos monitorados.

4.2 RESUMO DA ABORDAGEM EM SETE PASSOS

Essa abordagem de implementação pode ajudar as organizações a usar o Framework para estabelecer um programa forte de segurança cibernética ou para validar a eficácia de um programa existente. Ela permite que as organizações mapeiem seu programa para o Framework, identifiquem melhorias e comuniquem resultados. Pode incorporar e alinhar processos e ferramentas que a organização já está usando ou planeja usar.

Essa abordagem, como mostrada na Figura 1, pretende ser um processo contínuo, repetido de acordo com critérios definidos pela organização (como um período específico de tempo ou um tipo específico de evento) para abordar o ambiente de risco em evolução. A implementação dessa abordagem deve incluir um plano para comunicar o progresso às partes interessadas apropriadas, como a alta administração. Idealmente, esse processo seria integrado ao programa de gerenciamento de risco de uma organização. Além disso, cada etapa do processo deve fornecer feedback e validação para as etapas anteriores. A validação e o feedback fornecem um mecanismo para a melhoria do processo e podem aumentar sua eficácia geral e eficiência. Feedbacks abrangentes e bem estruturados, assim como planos de comunicação, são parte crítica de qualquer abordagem de gerenciamento de risco de segurança cibernética.

5 ABORDAGEM DA IMPLEMENTAÇÃO DO FRAMEWORK COM O MODELO DE MATURIDADE DE CAPACIDADE DE SEGURANÇA CIBERNÉTICA ABRATE

O Modelo de Maturidade de Capacidade de Cibersegurança ABRATE foi desenvolvido a partir do modelo C2M2 do Departamento de Energia dos Estados Unidos (DOE), com o objetivo de ajudar organizações de infraestrutura crítica a avaliar e potencialmente melhorar suas práticas de segurança cibernética. O modelo original foi ligeiramente adaptado pela ABRATE para as condições do setor elétrico brasileiro, e doravante será chamado apenas de “C2M2”

O C2M2 é usado como uma ferramenta de auto avaliação que orienta cada organização a identificar suas práticas de segurança cibernética e gerenciamento de risco, mapeá-las em níveis específicos de maturidade dentro do modelo, definir níveis de maturidade alvo e identificar lacunas e práticas potenciais que permitam à organização amadurecer com o tempo. O C2M2 abrange todas as práticas do Núcleo do Framework, auxiliando a organização a identificar seu Perfil Atual e estabelecer um Perfil Alvo.

Esta seção descreve os benefícios de se usar a abordagem C2M2 para a implementação do Framework, descreve brevemente o C2M2 em mais detalhes, e demonstra como ele pode suportar o Framework em sete etapas. Um mapeamento adaptado e detalhado do C2M2 para o Framework é fornecido no Apêndice A. Os itens do C2M2 adapatado pela ABRATE que foram mapeados ao Framework é fornecido no Apêndice B

5.1 BENEFÍCIOS DA ABORDAGEM C2M2 PARA A IMPLEMENTAÇÃO DO FRAMEWORK

Além de fornecer um processo passo-a-passo desenvolvido pela indústria e alinhado ao Framework, o C2M2 oferece os seguintes benefícios às empresas do setor elétrico interessadas em demonstrar sua implementação do Framework:

- ***Um objetivo comum:*** O objetivo do Framework e do C2M2 é ajudar as organizações de infraestrutura crítica a avaliar e potencialmente melhorar sua postura de segurança cibernética.
- ***Uso difundido:*** O C2M2 já foi adotado internacionalmente por muitas entidades do setor elétrico, o que permite que as organizações compartilhem voluntariamente conhecimentos e práticas eficazes usando terminologia comum.

- ***Possibilita o benchmarking em todo o setor:*** O amplo uso do modelo por cada empresa possibilita o benchmarking das capacidades de segurança cibernética do setor elétrico.
- ***Orientação descritiva para o Framework:*** O C2M2 fornece uma orientação descritiva genérica (o que fazer, mas não como fazer). Isso ajuda organizações de todos os tipos, estruturas e tamanhos a mapear práticas do C2M2 para Subcategorias do Framework. Além disso, o processo recomendado para usar o C2M2 é paralelo à abordagem do Framework de definir um Perfil Alvo, identificando e resolvendo lacunas.
- ***Cobertura completa das práticas do Framework:*** O mapeamento das práticas do C2M2 para Subcategorias mostra que o C2M2 aborda adequadamente os objetivos do Framework.
- ***Níveis de maturidade progressiva:*** O C2M2 usa níveis de indicador de maturidade que podem ajudar uma organização a acompanhar a progressão incremental e mensurável na maturidade das práticas de segurança cibernética.

5.2 VISÃO GERAL DO C2M2

O C2M2 está organizado em torno de dez domínios que abrangem a gama de práticas de segurança cibernética e gestão de risco utilizadas no setor elétrico, como mostra a Tabela 6:

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

Tabela 6 – Domínios e Abreviaturas do C2M2

Usando o C2M2, as organizações avaliam suas práticas atuais em cada domínio, cada qual

dividido em vários objetivos que o suportam (por exemplo, o domínio Gerenciamento de Riscos compreende três objetivos: Estabelecer a estratégia de gerenciamento de riscos de segurança cibernética, gerenciar riscos de segurança cibernética e atividades de gerenciamento). Os objetivos são compostos de uma ou mais práticas que demonstram que a organização está efetivamente atendendo seu nível definido de risco.

Todos os domínios possuem um objetivo comum, Atividades de Gerenciamento, que descreve as atividades que a organização realiza para *institucionalizar* as práticas específicas do domínio em toda a organização. Institucionalização refere-se ao quanto uma prática ou atividade está enraizada dentro da maneira como uma organização opera.

5.3 ALCANÇANDO E DEMONSTRANDO A MATURIDADE

Cada domínio do C2M2 inclui quatro Indicadores de Nível de Maturidade (Maturity Indicator Level - MILs): MIL0 (Não Realizado), MIL1 (Iniciado), MIL2 (Realizado) e MIL3 (Gerenciado). As organizações avançam progressivamente no nível de maturidade, melhorando: (1) a integridade, a perfeição ou o nível de desenvolvimento das práticas em um dado domínio; e (2) quão enraizadas ou institucionalizadas são as práticas nas operações da organização e na maneira de conduzir os negócios. As organizações alcançam um MIL quando realizam os objetivos e práticas de segurança cibernética específicos do domínio e as Atividades de Gerenciamento desse MIL. As organizações podem estabelecer uma meta de MIL para cada domínio para orientar sua melhoria na segurança cibernética.

5.4 ALAVANCANDO O C2M2 ABRATE PARA APOIAR A IMPLEMENTAÇÃO DO FRAMEWORK

Esta seção explica como a utilização do C2M2 aborda cada uma das etapas de implementação do Framework descritas na Seção 4. Os detalhes específicos para o C2M2 são exibidos em **negrito**.

Etapa 1: Priorizar e Definir o Escopo

Entradas	Atividades	Saídas
• Estratégia de gerenciamento de risco • Objetivos organizacionais e prioridades • Informações sobre ameaças • **C2M2**	• Determinar o escopo das operações que usarão o C2M2 para avaliar e potencialmente melhorar os recursos de segurança cibernética da organização.	• Escopo de uso do framework

As organizações iniciam uma autoavaliação C2M2 determinando o escopo ou subconjunto das operações da organização que serão avaliadas.

O C2M2 é flexível o suficiente para ser usado em qualquer escopo que uma organização escolher para a implementação do Framework, podendo incluir sistemas ou áreas de tecnologia que cruzam os limites da organização.

Etapa 2: Orientar

Entradas	Atividades	Saídas
• Escopo de uso do framework • Estratégia de gerenciamento de risco	• A organização identifica os sistemas e ativos dentro do escopo (por exemplo, pessoas, informações, tecnologia e instalações) e as referências normativas e informativas apropriadas (por exemplo, padrões, ferramentas, métodos e diretrizes de segurança cibernética e de riscos)	• Sistemas e ativos dentro do escopo • Requisitos de escopo (ou seja, regulatório, empresarial, organizacional) • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • **Método de avaliação: Autoavaliação do C2M2**

Uma vez tomada uma decisão de escopo, a organização identifica as informações, a tecnologia, as pessoas e as instalações abrangidas pelo escopo, os requisitos regulamentares aplicáveis e os padrões, ferramentas, métodos e diretrizes de segurança cibernética e de gerenciamento de riscos em uso.

Etapa 3: Criar um Perfil Atual

Entradas	Atividades	Saídas
• **Autoavaliação C2M2** • Sistemas e ativos dentro do escopo • Requisitos regulamentares no escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo	• **Realizar workshop de autoavaliação C2M2 com os participantes apropriados**	• **Relatório de avaliação C2M2** • **Nível de Implementação Atual (MIL**)

O C2M2 é normalmente aplicado por meio de um workshop que inclui pessoas-chave representando todos os ativos e funções no escopo. O workshop de autoavaliação C2M2 resulta em um Relatório de Avaliação (Pontuação) que pode servir como um Perfil Atual. Por meio de diálogo aberto e consenso, os participantes respondem a perguntas de avaliação sobre práticas em cada domínio. As respostas possíveis são “Atende” ou “Não Atende”.

O nível de implementação de cada subcategoria do Framework será definido com base nas respostas da avaliação das suas práticas. Para uma subcategoria ser avaliada como MIL1, todas as práticas de MIL1 devem estar atendidas. Para os níveis superiores, além das práticas daquele nível, é necessário que todas as práticas dos níveis anteriores também estejam atendidas.

Etapa 4: Realizar uma Avaliação de Risco

Entradas	Atividades	Saídas
• Escopo de uso do Framework • Estratégia de gerenciamento de risco • Abordagem de avaliação de risco definida pela organização • Requisitos regulamentares no escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • **Relatório de avaliação C2M2**	• Realizar a avaliação de risco no escopo	• Relatórios de avaliação de risco para o escopo

O C2M2 recomenda que as organizações usem o modelo como parte de um processo contínuo de gerenciamento de riscos corporativos que inclua avaliações de risco. Os resultados da avaliação de riscos são usados como entrada em todas as outras etapas de implementação do C2M2. Tanto o C2M2 como o Framework identificam a avaliação de risco como uma prática importante.

Etapa 5: Criar um Perfil Alvo

Entradas	Atividades	Saídas
• **Relatório de avaliação C2M2** • Objetivos organizacionais • Estratégia de gestão de risco • Relatórios de avaliação de riscos	• A Organização identifica o MIL ou práticas específicos que mitigarão o risco de acordo com seus objetivos	• Perfil Alvo do C2M2

O Relatório de Avaliação (Pontuação) C2M2 destaca áreas potenciais para melhoria. Por exemplo, dentro de qualquer domínio, as práticas que representam a realização do MIL1 são pré-requisitos para práticas que permitem a realização do MIL2. Todas as práticas devem estar presentes para alcançar o próximo MIL. O Relatório de Avaliação pode fornecer algumas ideias iniciais para o Perfil Alvo, chamando a atenção para a ausência de práticas de MILs inferiores. O relatório também deve incluir uma tabela “Resumo das lacunas identificadas”, que liste as perguntas da pesquisa que foram respondidas como “Não Atende” e é útil na definição de um Perfil Alvo.

A avaliação de risco pode ser usada junto com o Relatório de Avaliação para identificar MIL ou práticas específicas que mitigarão o risco de acordo com seus objetivos. Algumas práticas podem parecer necessárias com base na visão do Domínio para alcançar a próxima MIL, mas podem não fazer sentido para a organização com base em seu perfil de risco. Cada organização determina a meta de MIL e práticas que fazem sentido para cada domínio, de acordo com seus objetivos.

Etapa 6: Determinar, Analisar e Priorizar Lacunas

Entradas	Atividades	Saídas
• **Relatório de avaliação (pontuação) C2M2** • **Perfil Alvo do C2M2** • Objetivos organizacionais • Impacto na infraestrutura crítica • Lacunas e possíveis consequências • Restrições Organizacionais • Estratégia de gerenciamento de risco • Relatórios de avaliação de risco	• Analisar as lacunas entre o Perfil Atual e o Perfil Alvo no contexto da organização • Avalie possíveis conseqüências das lacunas • Determinar quais lacunas precisam de atenção • Identificar ações para solucionar lacunas • Realizar análise de custo-benefício das ações • Priorizar ações • Planejar a implementação de ações priorizadas	• Lacunas priorizadas e potenciais consequências • Plano de implementação priorizado

O Relatório de Avaliação (Pontuação) C2M2 permite que as organizações identifiquem as lacunas entre o Perfil Atual e o Perfil Alvo. A priorização das ações deve considerar como as lacunas afetam os objetivos organizacionais, a importância relativa desses objetivos, o custo de implementação das práticas e a disponibilidade de recursos.

A organização deve identificar os riscos que possam surgir como resultado das lacunas que não forem abordadas e decidir se essas lacunas podem ser mitigadas de outras maneiras. A organização pode optar por aceitar e gerenciar esses riscos. A prioridade das lacunas não resolvidas também pode ser reconsiderada se as autoavaliações do C2M2 forem realizadas periodicamente.

Etapa 7: Executar o Plano de Ação

Entradas	Atividades	Saídas
• Plano de implementação priorizado	• Implementar ações por prioridade • Monitorizar o progresso em relação ao plano • Reavaliar periodicamente ou em resposta a grandes mudanças	• Dados de acompanhamento do plano

6 RECOMENDAÇÕES ABRATE

O nível recomendado para implementação mínima de segurança cibernética é o menor nível de maturidade do C2M2 (MIL1) das subcategorias classificadas como prioritárias. O nível subsequente recomendado para implementação incluirá o menor nível de maturidade do C2M2 das subcategorias classificadas como recomendadas.

A ABRATE recomenda a execução periódica deste processo para melhorar continuamente o nível de segurança cibernética do setor elétrico.

7 REFERÊNCIAS

U.S. Department of Energy. **Cybersecurity Capability Maturity Model.** DOE, February 2014. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Energy. Cybersecurity **Capability Maturity Model Facilitator Guide.** DOE, February 2014. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-facilitator-guide-february-2014

U.S. Department of Energy. **Integrating Electricity Subsector Failures Scenarios into a Risk Assessment Methodology.** DOE, December 2013. http://energy.gov/oe/downloads/integrating-electricity-subsector-failure-scenarios-risk-assessment-methodology

U.S. Department of Energy. **Electricity Subsector Cybersecurity Capability Maturity**

Model. DOE, May 2012. http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

U.S. Department of Energy. **Electricity Subsector Cybersecurity Risk Management Process Guideline**. DOE, May 2012. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Security**. NIST, February 2014. http://www.nist.gov/cyberframework/index.cfm

Apêndice A – MAPEAMENTO DO C2M2 AO FRAMEWORK

Conforme discutido na Seção 5 deste guia, as organizações do setor elétrico que utilizam o C2M2 podem mapear suas práticas de C2M2 para as Funções, Categorias e Subcategorias do Framework de Segurança Cibernética para orientar suas decisões sobre o Perfil Alvo ou para demonstrar sua implementação do Framework.

O mapeamento apresentado na Tabela 7 abaixo apresenta uma visão abrangente de como o C2M2 complementa o Framework. É possível que uma organização que executa práticas C2M2 mapeadas para um resultado de estrutura específico possa determinar que algumas práticas C2M2 não satisfazem o resultado em um grau exigido por essa organização. As organizações que utilizam esse mapeamento devem, portanto, revisá-lo e garantir que ele se alinhe com suas necessidades.

As práticas C2M2 são denotadas pela abreviação do domínio, um hífen, o número do objetivo e a prática. Por exemplo, "ACM-1a" denota a prática A no Objetivo 1 do domínio Gerenciamento de Ativos, Mudanças e Configurações. As abreviaturas de domínio estão listadas na Tabela 6 da Seção 5. A lista completa de todas as práticas mapeadas do C2M2 é apresentada no Apêndice B.

Para permitir uma melhor adaptação às características do setor elétrico brasileiro, assim como facilitar a implantação pelas organizações, práticas complementares ao C2M2 foram criadas pela ABRATE e agrupadas em uma categoria denominada ABT

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
IDENTIFICAR (ID)	Gestão de Ativos (ID.AM):Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a	ID.AM-1: Dispositivos e sistemas físicos dentro da organização são inventariados	Prioritário	ACM-1a	ACM-1c	ACM-1e ACM-1f
		ID.AM-2: Plataformas e aplicativos de software dentro da organização são inventariados	Prioritário	ACM-1a	ACM-1c	ACM-1e ACM-1f

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	Categoria	Subcategoria		MIL 1	MIL 2	MIL 3
	organização atinja objetivos comerciais são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos de negócios e a estratégia de risco da organização.	ID.AM-3: Comunicação organizacional e fluxos de dados são mapeados	Prioritário	ABT-1a	RM-2g ABT-1b	ACM-1e
		ID.AM-4: Sistemas de informação externos são catalogados	Prioritário	EDM-1a	EDM-1c EDM-1e	EDM-1g RM-1c
		ID.AM-5: Recursos (ex: hardware, dispositivos, dados e software) são priorizados com base em sua classificação, importância e valor de negócio.	Prioritário	ACM-1a ACM-1b	ACM-1c ACM-1d	
		ID.AM-6: As funções e responsabilidades de segurança cibernética são estabelecidas.	Prioritário	WM-1a WM-1b	WM-1c	
	Ambiente de Negócios (ID.BE):A missão, os objetivos, as partes interessadas e as atividades da organização são compreendidas e priorizadas; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.	ID.BE-1: O papel da organização na cadeia de fornecimento é identificado e comunicado	Recomendável	EDM-1b	EDM-1d EDM-1f	EDM-1g RM-1c
		ID.BE-2: O papel da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado	Recomendável	EDM-1b	EDM-1d EDM-1f CPM-1c	EDM-1g RM-1c
		ID.BE-3: Prioridades para missão, objetivos e atividades organizacionais são estabelecidas e comunicadas	Recomendável		RM-3b	RM-1c
		ID.BE-4: Dependências e funções críticas para a entrega de serviços críticos são estabelecidas	Prioritário	ACM-1a ACM-1b EDM-1a	ACM-1c ACM-1d EDM-1c EDM-1e	ACM-1e ACM-1f RM-1c EDM-1g
		ID.BE-5: Requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos	Prioritário	IR-4a IR-4b IR-4c	IR-4e	
	Governança (ID.GV):As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulamentares, legais, de risco, ambientais e	ID.GV-1: Política de segurança da informação da organização é estabelecida	Recomendável		CPM-2g	CPM-5d RM-3e
		ID.GV-2: Os papéis e responsabilidades de segurança da informação são coordenados e alinhados com funções internas e parceiros externos	Recomendável	WM-1a WM-1b	WM-1c WM-2d WM-5b ISC-2b	WM-1e WM-1f WM-1g

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	Categoria	Subcategoria		MIL 1	MIL 2	MIL 3
	operacionais da organização são compreendidos e informam o gerenciamento do risco de segurança cibernética.	ID.GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo as obrigações de privacidade e das liberdades cívicas, são compreendidos e geridos	Prioritário	ABT-1c		CPM-2k IR-3n RM-3f ACM-4f IAM-3f TVM-3f SA-4f ISC-2f IR-5f EDM-3f WM-5f
		ID.GV-4: Processos de governança e gerenciamento de riscos tratam dos riscos de segurança cibernética	Prioritário	RM-2a RM-2b		RM-2h RM-3e RM-1c RM-1e
	Avaliação de Risco (ID.RA):A organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos.	ID.RA-1: As vulnerabilidades dos ativos são identificadas e documentadas	Prioritário	TVM-2a TVM-2b	TVM-2d TVM-2e TVM-2f	RM-1c RM-2j TVM-2i TVM-2j TVM-2k TVM-2l TVM-2m
		ID.RA-2: Informações de ameaças e vulnerabilidades são recebidas de fóruns e fontes de compartilhamento de informações	Recomendável	TVM-1a TVM-1b TVM-2a TVM-2b	TVM-2d	
		ID.RA-3: Ameaças internas e externas são identificadas e documentadas	Recomendável	TVM-1a TVM-1b	TVM-1d TVM-1e	RM-2j TVM-1j
		ID.RA-4: Os potenciais impactos ao negócio e as probabilidades são identificados	Prioritário	ABT-1d	TVM-1d TVM-1f	RM-1c TVM-1i

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	Prioritário	ABT-1e		RM-1c RM-2j TVM-2m
		ID.RA-6: As respostas ao risco são identificadas e priorizadas	Prioritário	RM-2a RM-2b	RM-2e TVM-1d	RM-1c RM-2j IR-3m
	Estratégia de Gerenciamento de Risco (ID.RM):As prioridades, restrições, tolerâncias de risco e premissas da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.	ID.RM-1: Processos de gestão de riscos são estabelecidos, gerenciados e acordados pelas partes interessadas da organização	Prioritário	RM-2a RM-2b	RM-1a RM-1b RM-2c RM-2d RM-2e RM-2g RM-3a RM-3b RM-3c RM-3d	RM-1c RM-1d RM-1e RM-2h RM-2j RM-3g RM-3h RM-3i
		ID.RM-2: A tolerância ao risco organizacional é determinada e aprovada	Prioritário	ABT-1f		RM-1c RM-1e
		ID.RM-3: A determinação da tolerância ao risco pela organização é subsidiada pelo seu papel na infraestrutura crítica e análise de risco específica do setor	Recomendável		RM-1b	RM-1c
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	IAM-1a IAM-1b IAM-1c	IAM-1d IAM-1e IAM-1f	RM-1c IAM-1g
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	Prioritário	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g
		PR.AC-3: O acesso remoto é gerenciado	Prioritário	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
		PR.AC-4: As permissões de acesso são gerenciadas, incorporando os princípios de menor privilégio e segregação de funções	Recomendável		IAM-2d	
		PR.AC-5: A integridade da rede é protegida, incorporando segregação de rede, quando apropriado	Prioritário	CPM-3a	CPM-3b CPM-3c	CPM-3d
	Conscientização e Treinamento (PR.AT): O pessoal e os parceiros da organização recebem educação sobre conscientização sobre segurança cibernética e são adequadamente treinados para desempenhar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com políticas, procedimentos e acordos relacionados.	PR.AT-1: Todos os usuários são informados e treinados	Prioritário	WM-3a WM-4a	WM-3b WM-3c WM-3d	WM-3g WM-3h WM-3i
		PR.AT-2: Usuários privilegiados entendem papéis e responsabilidades	Prioritário	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-3: Partes interessadas de terceiros (fornecedores, clientes, parceiros) entendem papéis e responsabilidades	Prioritário	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-4: A Alta Administração entende seus papéis e responsabilidades	Prioritário	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-5: O pessoal de segurança física e cibernética compreende os papéis e responsabilidades	Prioritário	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
	Segurança de dados (PR.DS): As informações e os registros (dados) são gerenciados de maneira	PR.DS-1: Os dados armazenados são protegidos	Prioritário	TVM-1c TVM-2c		
		PR.DS-2: O transporte de dados é protegido	Prioritário	TVM-1c TVM-2c		

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	Categoria	Subcategoria		MIL 1	MIL 2	MIL 3
	consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade das informações.	PR.DS-3: Os ativos são formalmente gerenciados durante a implantação, transferência e alienação	Prioritário	ACM-3a ACM-3b	ACM-3c ACM-3d ACM-4a ACM-4b ACM-4c ACM-4d	ACM-3f ACM-4e ACM-4f ACM-4g
		PR.DS-4: Capacidade adequada para assegurar que a disponibilidade seja mantida	Recomendável	TVM-1c TVM-2c	CPM-3b	
		PR.DS-5: Proteções contra vazamentos de dados são implementadas	Recomendável	TVM-1c TVM-2c	CPM-3b	TVM-2n
		PR.DS-6: Mecanismos de verificação de integridade são usados para verificar software, firmware e integridade de informações	Recomendável		SA-2e	SA-2i
		PR.DS-7: Os ambientes de desenvolvimento, teste e homologação são separados dos ambientes de produção	Recomendável		ACM-3c	ACM-3e
	Processos e Procedimentos de Proteção da Informação (PR.IP): As políticas de segurança (que tratam de propósito, escopo, funções, responsabilidades, comprometimento de gerenciamento e coordenação entre entidades organizacionais), processos e	PR.IP-1: Uma configuração de linha de base (baseline) de sistemas de tecnologia da informação / controle industrial é criada e mantida	Prioritário	ACM-2a ACM-2b	ACM-2c	ACM-2d ACM-2e
		PR.IP-2: Um ciclo de vida de desenvolvimento de sistemas é implementado	Recomendável		ACM-3d	
		PR.IP-3: Processos de controle de mudança de configuração estão em vigor	Prioritário	ACM-3a ACM-3b	ACM-3c ACM-3d ACM-4a	ACM-3e ACM-3f ACM-4e
		PR.IP-4: Backups de informações são realizados, mantidos e testados periodicamente	Prioritário	IR-4a IR-4b		
		PR.IP-5: As políticas e regulamentações relativas ao ambiente operacional físico dos ativos organizacionais são atendidas	Recomendável			ACM-4f RM-3f

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
	procedimentos são mantidas e usadas para gerenciar a proteção de ativos e sistemas de informação.	PR.IP-6: Os dados são destruídos de acordo com a política	Recomendável		ACM-3d	
		PR.IP-7: Os processos de proteção são continuamente aprimorados	Recomendável			CPM-1g
		PR.IP-8: A efetividade das tecnologias de proteção é compartilhada com as partes apropriadas	Recomendável	ISC-1a ISC-1b	ISC-1c ISC-1d ISC-1e ISC-1f ISC-1g ISC-2b	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l
		PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão implementados e gerenciados	Prioritário	IR-4c	IR-3f IR-4d IR-4f IR-5a IR-5b IR-5d TVM-1d	IR-3k IR-3m IR-4i IR-4j IR-5e IR-5f IR-5g IR-5h IR-5i RM-1c
		PR.IP-10: Planos de resposta e recuperação são testados	Recomendável		IR-3e IR-4f	IR-3k IR-4i IR-4j
		PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, de aprovisionamento, triagem de pessoal)	Recomendável	WM-2a WM-2b	WM-2c WM-2d	WM-2e WM-2f WM-2g WM-2h
		PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	Prioritário	TVM-2c	TVM-3a	TVM-3e
		PR.IP-A1: A gestão do ciclo de vida de equipamentos é implementada	Recomendável		ACM-3d	

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
	Manutenção (PR.MA):Manutenção e reparos de controles industriais e componentes do sistema de informação são realizados de forma consistente com políticas e procedimentos.	PR.MA-1: Manutenção e reparo de ativos organizacionais são realizados e registrados em tempo hábil, com ferramentas aprovadas e controladas	Recomendável	ACM-3b	ACM-4c	ACM-3f
		PR.MA-2: A manutenção remota de ativos da organização é aprovada, registrada e executada de maneira a impedir o acesso não autorizado	Recomendável	SA-1a IR-1c IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h
	Tecnologia de proteção (PR.PT): Soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência de sistemas e ativos, consistentes com políticas, procedimentos e acordos relacionados.	PR.PT-1: Os registros de auditoria e registros de log são determinados, documentados, implementados e revistos de acordo com as políticas	Prioritário	SA-1a SA-2a	SA-1b SA-1c SA-2e SA-4a	SA-1d SA-1e SA-3d SA-4e SA-4f SA-4g
		PR.PT-2: A mídia removível é protegida e seu uso é restrito de acordo com a política	Prioritário	IAM-2a IAM-2b IAM-2c		IAM-3e IAM-3f
		PR.PT-3: O acesso a sistemas e ativos é controlado, incorporando o princípio da menor funcionalidade	Prioritário	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h IAM-2i
		PR.PT-4: As redes de comunicações e controle estão protegidas	Prioritário	CPM-3a	CPM-3b CPM-3c	CPM-3d
DETECTAR (DE)	Anomalias e Eventos (DE.AE):A atividade anômala é detectada em tempo hábil e o impacto potencial dos eventos é compreendido.	DE.AE-1: Uma linha de base (baseline) de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	Prioritário	SA-2a		
		DE.AE-2: Os eventos detectados são analisados para entender os alvos e métodos de ataque	Recomendável			IR-1f IR-2i IR-3h

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
		DE.AE-3: Os dados do evento são agregados e correlacionados a partir de várias fontes e sensores	Recomendável		IR-1e	IR-1f IR-2i
		DE.AE-4: O impacto dos eventos é determinado	Prioritário	IR-2b	IR-2d TVM-1d	IR-2g RM-2j
		DE.AE-5: Limites de alerta de incidentes são estabelecidos	Prioritário	IR-2a	IR-2d TVM-1d SA-2d	IR-2g RM-2j
	Monitoramento Contínuo de Segurança (DE.CM):Os sistemas de informação e os ativos são monitorados em intervalos discretos para identificar eventos de segurança cibernética e verificar a eficácia de medidas de proteção.	DE.CM-1: A rede é monitorada para detectar possíveis eventos de segurança cibernética	Prioritário	SA-2a SA-2b	SA-2e SA-2f TVM-1d	SA-2g SA-2i
		DE.CM-2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética	Recomendável	SA-2a SA-2b	SA-2e	SA-2i
		DE.CM-3: As atividades são monitoradas para detectar possíveis eventos de segurança cibernética	Recomendável	SA-2a SA-2b	SA-2e	SA-2i
		DE.CM-4: Código malicioso é detectado	Recomendável	SA-2a SA-2b	SA-2e CPM-4a	SA-2i
		DE.CM-5: O código móvel (proveniente de fontes remotas e executado localmente) não autorizado é detectado	Recomendável	SA-2a SA-2b	SA-2e	SA-2h SA-2i
		DE.CM-6: A atividade de provedor de serviço externo é monitorada para detectar possíveis eventos de segurança cibernética	Prioritário	EDM-2a SA-2a SA-2b	SA-2e	EDM-2j EDM-2n
		DE.CM-7: Monitoramento de pessoal, de conexões, de dispositivos e de softwares não autorizados é realizado	Prioritário	SA-2a SA-2b	SA-2e SA-2f TVM-1d	SA-2g SA-2i
		DE.CM-8: Buscas por vulnerabilidades são executadas	Recomendável		TVM-2e	TVM-2i TVM-2j TVM-2k RM-1c

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	**Categoria**	**Subcategoria**		**MIL 1**	**MIL 2**	**MIL 3**
	Processos de Detecção (DE.DP):Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização adequada e oportuna de eventos anômalos.	DE.DP-1: Os papéis e responsabilidades pela detecção são bem definidos	Prioritário	WM-1a	WM-1d	WM-1f
		DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis	Prioritário	ABT-1g	IR-1d IR-5a TVM-1d	IR-1g IR-5f RM-1c RM-2j
		DE.DP-3: os processos de detecção são testados	Recomendável		IR-3e	IR-3j
		DE.DP-4: Informações de detecção de evento são comunicadas às partes apropriadas	Prioritário	IR-1b IR-3c ISC-1a	ISC-1c ISC-1d	IR-3n ISC-1h ISC-1j
		DE.DP-5: Os processos de detecção são continuamente aprimorados	Recomendável			IR-3h IR-3k
RESPONDER (RS)	Planejamento de Respostas (RS.RP):Processos e procedimentos de resposta são executados e mantidos, para garantir a resposta oportuna aos eventos de segurança cibernética detectados.	RS.RP-1: O plano de resposta a incidentes é executado durante ou após um evento	Prioritário	ABT-1h	IR-3d	
	Comunicações (RS.CO):As atividades de resposta são coordenadas com as partes interessadas internas e externas, conforme apropriado.	RS.CO-1: Papéis e procedimentos quando uma resposta é necessária são conhecidos	Prioritário	IR-3a	IR-5b	
		RS.CO-2: Eventos são relatados de forma consistente com os critérios estabelecidos	Recomendável	IR-1a IR-1b		
		RS.CO-3: As informações são compartilhadas de maneira consistente com os planos de resposta	Recomendável	ISC-1a ISC-1b	IR-3d ISC-1c ISC-1d	IR-3i IR-3l
		RS.CO-4: A coordenação das atividades de resposta com as partes interessadas ocorre de forma consistente com os planos de resposta	Recomendável		IR-3d IR-5b	

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	Categoria	Subcategoria		MIL 1	MIL 2	MIL 3
		RS.CO-5: Compartilhamento voluntário de informações ocorre com partes interessadas externas para alcançar um maior conhecimento da situação de segurança cibernética	Recomendável	ISC-1a	ISC-1c ISC-1d ISC-1e ISC-1f	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l
	Análise (RS.AN):A análise é conduzida para assegurar uma resposta adequada e apoiar as atividades de recuperação.	RS.AN-1: Notificações de sistemas de detecção são investigadas	Prioritário	IR-1c	IR-1e	IR-1f
		RS.AN-2: O impacto do incidente é entendido	Prioritário	IR-2a	IR-2d TVM-1d	IR-2g RM-2j
		RS.AN-3: Análise forense é realizada	Recomendável		IR-3d	IR-3h IR-3i
		RS.AN-4: Os incidentes são categorizados de forma consistente com os planos de gestão e resposta a incidentes	Prioritário	IR-2a	IR-1d IR-1e	
	Mitigação (RS.MI):As atividades são realizadas para impedir a expansão de um evento, mitigar seus efeitos e erradicar o incidente.	RS.MI-1: Incidentes são contidos	Prioritário	IR-3b		
		RS.MI-2: Incidentes são mitigados	Prioritário	IR-3b		
		RS.MI-3: Vulnerabilidades não previstas são mitigadas ou documentadas como riscos aceitos	Prioritário	TVM-2c	TVM-2f TVM-2g	RM-2j TVM-2m TVM-2n
	Melhorias (RS.IM):As atividades de resposta organizacional são aprimoradas pela incorporação de lições aprendidas de atividades de detecção / resposta atuais e anteriores.	RS.IM-1: Planos de resposta incorporam lições aprendidas	Recomendável			IR-3h
		RS.IM-2: As estratégias de resposta são atualizadas	Recomendável			IR-3h IR-3k

Núcleo do Framework			Prioridade	Práticas C2M2		
Função	Categoria	Subcategoria		MIL 1	MIL 2	MIL 3
RECUPERAR (RC)	Planejamento de Recuperação (RC.RP):Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração em tempo hábil de sistemas ou ativos afetados por eventos de segurança cibernética.	RC.RP-1: O plano de recuperação é executado durante ou depois de um evento	Prioritário	IR-3b	IR-3d	IR-3o IR-4k
	Melhorias (RC.IM):O planejamento e os processos de recuperação são aprimorados pela incorporação de lições aprendidas em atividades futuras.	RC.IM-1: Planos de recuperação incorporam lições aprendidas	Recomendável			IR-3h IR-4i IR-3k
		RC.IM-2: As estratégias de recuperação são atualizadas	Recomendável			IR-3h IR-3k
	Comunicações (RC.CO):As atividades de restauração são coordenadas com partes internas e externas.	RC.CO-1: Relações públicas são gerenciadas	Recomendável			RM-1c
		RC.CO-2: Reputação após um evento ser reparado	Recomendável		IR-3d	
		RC.CO-3: As atividades de recuperação são comunicadas às partes interessadas internas e às equipes executivas e gerenciais	Prioritário	IR-3c	IR-3d	

Tabela 7 – Mapeamento do C2M2 ao Framework

Apêndice B **– DESCRIÇÃO DAS PRÁTICAS MAPEADAS DO C2M2**

Os itens abaixo descritos contemplam apenas uma parte do C2M2, relativa às práticas que foram mapeadas no Framework. Para uma completa visão do C2M2 consulte a documentação oficial do Departamento de Energia dos EUA (DOE).

GERENCIAMENTO DE RISCOS (RM)

RM-1: Estabelecer a estratégia de gerenciamento de riscos de segurança cibernética

a. Existe uma estratégia documentada de gerenciamento de riscos de segurança cibernética.
b. A estratégia fornece uma abordagem para a priorização de riscos, incluindo a consideração do impacto.
c. Critérios de risco organizacional (critérios objetivos que a organização usa para avaliar, categorizar e priorizar riscos operacionais com base no impacto, tolerância ao risco e abordagens de resposta ao risco) estão definidos e disponíveis.
d. A estratégia de gerenciamento de riscos é atualizada periodicamente para refletir o ambiente atual de ameaças.
e. Uma taxonomia de risco específica da organização é documentada e é usada em atividades de gerenciamento de risco.

RM-2: Gerenciar o risco de segurança cibernética

a. Os riscos de segurança cibernética são identificados, pelo menos de forma ad hoc.
b. Os riscos identificados são mitigados, aceitos, tolerados ou transferidos, pelo menos de maneira ad hoc.
c. Avaliações de risco são realizadas para identificar riscos de acordo com a estratégia de gerenciamento de riscos.
d. Riscos identificados são documentados.
e. Os riscos identificados são analisados para priorizar as atividades de resposta de acordo com a estratégia de gerenciamento de riscos.
g. A análise de risco é subsidiada pela arquitetura de rede (TI e/ou TO).
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.
j. Um registro de riscos (um repositório estruturado de riscos identificados) é usado para

suportar atividades de gerenciamento de riscos.

RM-3: Atividades de gerenciamento

a. Práticas documentadas são seguidas para atividades de gerenciamento de risco.
b. As partes interessadas, para as atividades de gerenciamento de riscos, são identificadas e envolvidas.
c. Recursos adequados (pessoas, financeiros e ferramentas) são fornecidos para apoiar as atividades de gerenciamento de risco.
d. Normas e/ou diretrizes foram identificadas para informar as atividades de gerenciamento de riscos.
e. As atividades de gerenciamento de riscos são guiadas por políticas documentadas ou outras diretrizes organizacionais.
f. As políticas de gerenciamento de riscos incluem requisitos de conformidade para padrões e/ou diretrizes especificados.
g. As atividades de gerenciamento de risco são revisadas periodicamente para garantir a conformidade com a política.
h. A responsabilidade e autoridade para o desempenho das atividades de gerenciamento de risco são atribuídas às pessoas.
i. O pessoal, que executa atividades de gerenciamento de riscos, possui as habilidades e os conhecimentos necessários para executar suas responsabilidades atribuídas.

ATIVOS, MUDANÇAS E GERENCIAMENTO DE CONFIGURAÇÕES (ACM)

ACM-1: Gerenciar Inventário de Ativos

a. Existe um inventário de TO e ativos de TI que são importantes para a entrega da função; gestão do inventário pode ser ad hoc.
b. Há um inventário de ativos de informação que são importantes para a entrega da função (por exemplo, pontos de ajuste do SCADA, informações do cliente, dados financeiros); gestão do inventário pode ser ad hoc.
c. Atributos de inventário incluem informações para dar suporte à estratégia de segurança cibernética (por exemplo: local, proprietário do ativo, requisitos de segurança aplicáveis, dependências de serviço, contratos de nível de serviço e conformidade de ativos com os padrões relevantes do setor).
d. Os bens inventariados são priorizados com base em sua importância para a entrega da função.
e. Existe um inventário para todos os ativos conectados de TI e TO relacionados à entrega da função.
f. O inventário de ativos é atualizado (conforme definido pela organização).

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 ativos sejam configurados de forma semelhante.

b. Baselines de configuração são usadas, pelo menos de maneira ad hoc, para configurar ativos na implantação.

c. O design de baselines de configuração inclui objetivos de segurança cibernética.

d. A configuração dos ativos é monitorada quanto à consistência com as baselines ao longo do ciclo de vida dos ativos.

e. As baselines de configuração são revisadas e atualizadas em uma frequência definida organizacionalmente.

ACM-3: Gerenciar mudança nos ativos

a. As alterações nos ativos inventariados são avaliadas, pelo menos de maneira ad hoc, antes de serem implementadas.

b. As alterações nos ativos inventariados são registradas, pelo menos de maneira ad hoc.

c. As alterações nos ativos são testadas, sempre que possível, antes de serem implantadas (em ambiente apropriado).

d. As práticas de gerenciamento de mudanças abordam o ciclo de vida completo dos ativos (isto é, Identificação da necessidade, projeto, aquisição, comissionamento e implantação, operação e manutenção, modificação ou atualização, descomissionamento e descarte)

e. As alterações nos ativos são testadas quanto ao impacto na segurança cibernética antes de serem implantadas (em ambiente apropriado).

f. Os registros de alterações devem incluir informações sobre modificações que afetam os requisitos de segurança cibernética dos ativos (disponibilidade, integridade, confidencialidade).

ACM-4: Atividades de Gestão

a. Práticas documentadas são seguidas para atividades de inventário e de gerenciamento de configuração e de mudanças de ativos.

b. As partes interessadas no inventário e no gerenciamento de configuração e de mudanças de ativos são identificadas e envolvidas.

c. Recursos adequados (pessoas, financeiro e ferramentas) são fornecidos para suportar atividades de inventário e de gerenciamento de configuração e de mudanças de ativos.

d. Padrões e/ou diretrizes são identificados para subsidiar as atividades de inventário e de gerenciamento de configuração e de mudanças de ativos.

e. As atividades de inventário e de gerenciamento de configuração e de mudanças de ativos são orientadas por políticas documentadas ou outras diretrizes organizacionais.

f. As políticas de inventário e de gerenciamento de configuração e de mudanças de ativos incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

g. As atividades de inventário e de gerenciamento de configuração e de mudanças de ativos são revisadas periodicamente para assegurar a conformidade com a política.

GERENCIAMENTO DE IDENTIDADE E ACESSO (IAM)

IAM-1: Estabelecer e manter identidades

a. As identidades são provisionadas, pelo menos de maneira ad hoc, para funcionários e outras entidades (por exemplo: serviços, dispositivos) que exigem acesso a ativos (observe que isso não exclui identidades compartilhadas).

b. As credenciais são emitidas, pelo menos de maneira ad hoc, para funcionários e outras entidades que exigem acesso a ativos (por exemplo, senhas, cartões inteligentes, certificados, chaves).

c. As identidades são revogadas, pelo menos de maneira ad hoc, quando não são mais necessárias.

d. Os repositórios de identidade são revisados e atualizados periodicamente para garantir a validade (ou seja, para garantir que as identidades ainda precisem de acesso).

e. As credenciais são revisadas periodicamente para garantir que estejam associadas às pessoas ou entidade correta.

f. As identidades são desprovisionadas, dentro dos limites de tempo definidos pela organização, quando não são mais necessários.

g. Os requisitos para credenciais são informados pelos critérios de risco da organização (por exemplo: credenciais multifatores para acesso de maior risco) (RM-1c).

IAM-2: Controle de Acesso

a. Os requisitos de acesso, incluindo os de acesso remoto, são determinados pelo menos de maneira ad hoc. Obs.: Os requisitos de acesso estão associados a ativos e fornecem orientação para quais tipos de entidades têm permissão para acessar o ativo, os limites de acesso permitido e parâmetros de autenticação.

b. O acesso é concedido às identidades, pelo menos de forma ad hoc, com base nos requisitos.

c. O acesso é revogado, pelo menos de maneira ad hoc, quando não é mais necessário.

d. Requisitos de acesso incorporam os princípios de menor privilégio e segregação de funções.

e. Solicitações de acesso são revisadas e aprovadas pelo proprietário do ativo.

f. Privilégios de administrador, acesso administrativo, acesso de emergência e contas compartilhadas recebem exame minucioso e monitoramento adicionais.

g. Os privilégios de acesso são revisados e atualizados para garantir a validade, em uma frequência definida organizacionalmente.

h. O acesso aos ativos é concedido, pelo proprietário do ativo, com base no risco para a função.

i. Tentativas de acesso anormais são monitoradas como indicadores de eventos de segurança cibernética.

IAM-3: Atividades de Gerenciamento

e. As atividades de gerenciamento de acesso e identidade são guiadas por políticas documentadas ou outras diretrizes organizacionais.

f. As políticas de gerenciamento de acesso e identidade incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

GESTÃO DE AMEAÇAS E VULNERABILIDADES (TVM)

TVM-1: Identificar e responder à ameaças

a. Fontes de informação para apoiar atividades de gerenciamento de ameaças (associados do setor, fornecedores, diretrizes federais, orgãos reguladores), são identificadas pelo menos de maneira ad hoc.

b. Informações de ameaça de segurança cibernética são coletadas e interpretadas para a função, pelo menos de maneira ad hoc.

c. Ameaças que são consideradas importantes para a função (por exemplo: implementar controles de mitigação, monitorar status de ameaça) são endereçadas pelo menos de maneira ad hoc.

d. Um perfil de ameaça para a função é estabelecido, o que inclui a caracterização da provável intenção, capacidade e alvo das ameaças à função.

e. As fontes de informações de ameaças que abordam todos os componentes do perfil de ameaça são priorizadas e monitoradas.

f. As ameaças identificadas são analisadas e priorizadas.

i. Análise e priorização de ameaças são subsidiadas pelos critérios de risco da função (ou organização) (RM-1c).

j. Informações sobre ameaças são adicionadas ao registro de riscos (RM-2j).

TVM-2: Reduzir Vulnerabilidades de Cibersegurança

a. As fontes de informação para dar suporte à descoberta de vulnerabilidades de segurança cibernética (por exemplo: CERT, associações do setor, fornecedores, diretrizes federais, avaliações internas) são identificadas pelo menos de maneira ad hoc.

b. As informações de vulnerabilidade de segurança cibernética são coletadas e interpretadas

para a função, pelo menos de maneira ad hoc.

c. Vulnerabilidades de segurança cibernética, que são consideradas importantes para a função, são abordadas (por exemplo, implementar controles de mitigação, aplicar patches de segurança cibernética), pelo menos de maneira ad hoc.

d. As fontes de informação de vulnerabilidade de segurança cibernética, que tratam de todos os ativos importantes para a função, são monitoradas.

e. Avaliações de vulnerabilidade de segurança cibernética são realizadas (por exemplo, revisões de arquitetura, testes de penetração em laboratório, exercícios de segurança cibernética, ferramentas de identificação de vulnerabilidades).

f. As vulnerabilidades de segurança cibernética identificadas são analisadas e priorizadas [por exemplo: Forum of Incident Response and Security Teams (FIRST), CVSS (Common Vulnerability Scoring System) podem ser usados para patches; diretrizes internas podem ser usadas para priorizar outros tipos de vulnerabilidades].

g. As vulnerabilidades de segurança cibernética são abordadas de acordo com a prioridade atribuída.

i. As avaliações de vulnerabilidade de segurança cibernética são realizadas para todos os ativos importantes para a entrega da função, em uma frequência definida pela organização.

j. As avaliações de vulnerabilidade de segurança cibernética são informadas pelos critérios de risco da função (ou organização) (RM-1c).

k. As avaliações de vulnerabilidade de segurança cibernética são realizadas por partes independentes das operações da função.

l. Análise e priorização de vulnerabilidades de segurança cibernética são informadas pelos critérios de risco da função (ou organização) (RM-1c).

m. Informações de vulnerabilidade de segurança cibernética são adicionadas ao registro de riscos (RM-2j).

n. As atividades de monitoramento de risco validam as respostas às vulnerabilidades de segurança cibernética (por exemplo, implantação de patches ou outras atividades).

TVM-3: Atividades de Gerenciamento

a. Práticas documentadas são seguidas para atividades de gerenciamento de ameaças e vulnerabilidades.

e. As atividades de gerenciamento de ameaças e vulnerabilidades são guiadas por políticas documentadas ou outras diretrizes organizacionais.

f. As políticas de gerenciamento de ameaças e vulnerabilidades incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

CONSCIÊNCIA SITUACIONAL (SA)

SA-1: Registro

a. O registro (log) está ocorrendo, pelo menos de maneira ad hoc, para ativos importantes para a função, sempre que possível.

b. Os requisitos de registro (log) foram definidos para todos os ativos importantes para a função (por exemplo: escopo de atividade e cobertura de ativos, requisitos de segurança cibernética [confidencialidade, integridade, disponibilidade]).

c. Dados de registro (log) estão sendo agregados dentro da função.

d. Requisitos de registro (log) são baseados no risco para a função.

e. Os dados de registro (log) suportam outros processos comerciais e de segurança (por exemplo: resposta a incidentes, gerenciamento de ativos).

SA-2: Realizar Monitoramento

a. As atividades de monitoramento de segurança cibernética (por exemplo: revisões periódicas de dados de log) são realizadas pelo menos de uma maneira ad hoc.

b. Os ambientes operacionais são monitorados, pelo menos de maneira ad hoc, para comportamentos anormais que podem indicar um evento de segurança cibernética.

d. Alarmes e alertas são configurados para auxiliar na identificação de eventos de segurança cibernética (IR-1b).

e. Indicadores de atividade anormal foram definidos e monitorados em todo o ambiente operacional.

f. As atividades de monitoramento estão alinhadas com o perfil de ameaça da função (TVM-1d).

g. Os requisitos de monitoramento são baseados no risco para a função.

h. O monitoramento é integrado a outros processos comerciais e de segurança (por exemplo: resposta a incidentes, gerenciamento de ativos).

i. Monitoramento contínuo é realizado em todo o ambiente operacional para identificar atividades anormais.

SA-3: Estabelecer e Manter a Panorama Operacional Comum (Common Operating Picture - COP)

d. Os dados de monitoramento são agregados para fornecer uma compreensão quase em tempo real do estado de segurança cibernética para que a função melhore a Panorama Operacional Comum (Common Operating Picture. COP). *

SA-4: Atividades de Gerenciamento

a. Práticas documentadas são seguidas para registro, monitoramento e atividades de COP.

e. As atividades de registro, monitoramento e COP são guiadas por políticas documentadas ou outras diretrizes organizacionais.

f. As políticas de registro, monitoramento e COP incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

g. As atividades de registro, monitoramento e COP são revisadas periodicamente para assegurar a conformidade com as políticas.

COMPARTILHAMENTO DE INFORMAÇÕES E COMUNICAÇÕES (ISC)

ISC-1: Compartilhar Informações de Segurança Cibernética

a. As informações são coletadas e fornecidas a indivíduos e/ou organizações selecionados, pelo menos de maneira ad hoc.

b. A responsabilidade pelas obrigações de relatórios de segurança cibernética (por exemplo: relatórios internos, formulários específicos, aplicação da lei) é atribuída às pessoas pelo menos de forma ad hoc.

c. As partes interessadas no compartilhamento de informações são identificadas com base em sua relevância para a operação contínua da função (por exemplo, empresas conectadas, fornecedores, organizações setoriais, orgãos reguladores, entidades internas).

d. As informações são coletadas e fornecidas às partes interessadas identificadas, que compartilham informações.

e. As fontes técnicas, que podem ser consultadas sobre questões de segurança cibernética, são identificadas.

f. São estabelecidas e mantidas condições (provisões) para permitir o compartilhamento seguro de informações sensíveis ou sigilosas.

g. As práticas de compartilhamento de informações abordam operações padrão e operações de emergência.

h. O compartilhamento de informações das partes interessadas são identificados com base no interesse compartilhado e risco para a infraestrutura crítica.

i. A função ou a organização participa com compartilhamento de informação e centros de análise.

j. Os requisitos de compartilhamento de informações foram definidos para a função e abordam a disseminação oportuna das informações de segurança cibernética.

k. Existem procedimentos para analisar e desfazer conflitos entre as informações recebidas.

l. Foi estabelecida uma rede de relações internas e externas de confiança (formais e/ou informais) para avaliar e validar informações sobre eventos cibernéticos.

ISC-2: Atividades de Gerenciamento

b. As partes interessadas para atividades de compartilhamento de informações são identificadas e envolvidas.

f. As políticas de compartilhamento de informações incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

RESPOSTA A EVENTOS E INCIDENTES, CONTINUIDADE DAS OPERAÇÕES (IR)

IR-1: Detectar eventos de segurança cibernética

a. Existe um ponto de contato (pessoa ou função) para quem os eventos de segurança cibernética podem ser relatados.

b. Os eventos de cibersegurança detectados são relatados, pelo menos de maneira ad hoc.

c. Os eventos de segurança cibernética são registrados e rastreados, pelo menos de maneira ad hoc.

d. São estabelecidos critérios para detecção de eventos de segurança cibernética (por exemplo: o que constitui um evento, onde procurar eventos).

e. Existe um repositório onde os eventos de segurança cibernética são registrados com base nos critérios estabelecidos.

f. As informações sobre eventos estão correlacionadas com a análise de incidentes de suporte, identificando padrões, tendências e outros recursos comuns.

g. As atividades de detecção de eventos de segurança cibernética são ajustadas com base nas informações do registro de riscos da organização (RM-2j) e no perfil de ameaças (TVM-1d) para ajudar a detectar ameaças conhecidas e monitorar os riscos identificados.

IR-2: Agravamento de eventos de segurança cibernética e declarar incidentes.

a. Critérios para agravamento de eventos de segurança cibernética são estabelecidos, incluindo critérios de declaração de incidentes de segurança cibernética, pelo menos de uma maneira ad hoc.

b. Os eventos de segurança cibernética para dar suporte ao agravamento e à declaração de incidentes de segurança cibernética são analisados pelo menos de maneira ad hoc.

d. Critérios para agravamento de eventos de segurança cibernética, incluindo critérios de incidentes de segurança cibernética, são estabelecidos com base no impacto potencial para a função.

g. Os critérios para agravamento de eventos de segurança cibernética, incluindo critérios de declaração de incidentes de segurança cibernética, são ajustados de acordo com as informações do registro de riscos da organização (RM-2j) e perfil de ameaças (TVM-1d).

i. Eventos agravados de segurança cibernética e incidentes declarados são correlacionados

para suportar a descoberta de padrões, tendências e outros recursos comuns.

IR-3: Responder a incidentes e eventos agravados de segurança cibernética

a. A equipe de resposta a incidentes e eventos de segurança cibernética é identificada e as funções são atribuídas, pelo menos de maneira ad hoc.

b. As respostas aos eventos e incidentes de segurança cibernética agravados são implementadas, pelo menos de maneira ad hoc, para limitar o impacto na função e restaurar as operações normais.

c. O relato de eventos e incidentes agravados de segurança cibernética (por exemplo, relatórios internos, formulários específicos) é realizado pelo menos de maneira ad hoc.

d. A resposta aos eventos e incidentes de segurança cibernética é realizada de acordo com procedimentos definidos que abordam todas as fases do ciclo de vida do incidente (por exemplo: triagem, manuseio, comunicação, coordenação e fechamento)

e. Os planos de resposta a incidentes e eventos de cibersegurança são testados com periodicidade definida pela organização.

f. Os planos de resposta a incidentes e eventos de segurança cibernética abordam os ativos de TO e TI importantes para a entrega da função.

h. O evento de segurança cibernética e a análise da causa-raiz do incidente e atividades de lições aprendidas são realizadas, e ações corretivas são tomadas.

i. O evento de segurança cibernética e as respostas a incidentes são coordenados com as autoridades legais e outras entidades governamentais, conforme apropriado, incluindo o apoio à coleta e preservação de evidências.

j. A equipe de resposta a incidentes e eventos de segurança cibernética participa de exercícios conjuntos de segurança cibernética com outras organizações (por exemplo: tabela, incidentes simulados).

k. Os planos de resposta a incidentes e eventos de segurança cibernética são revisados e atualizados com periodicidade definida pela organização.

l. As atividades de resposta a eventos e incidentes de segurança cibernética são coordenadas com entidades externas relevantes.

m. Os planos de resposta a incidentes e eventos de segurança cibernética estão alinhados com os critérios de risco da função (RM-1c) e o perfil de ameaças (TVM-1d).

n. Políticas e procedimentos para relatar informações de incidentes e eventos de segurança cibernética às autoridades designadas em conformidade com as leis, regulamentos e acordos contratuais aplicáveis.

o. Os recursos restaurados são configurados adequadamente e as informações de inventário são atualizadas após a execução dos planos de resposta.

IR-4: Plano de Continuidade

a. As atividades necessárias para sustentar operações mínimas da função são identificadas, pelo menos de maneira ad hoc.

b. A seqüência de atividades necessárias para retornar a função à operação normal é identificada, pelo menos de maneira ad hoc.

c. Os planos de continuidade são desenvolvidos, pelo menos de maneira ad hoc, para manter e restaurar a operação da função.

d. Análises de impacto nos negócios informam o desenvolvimento de planos de continuidade.

e. Os requisitos de Recovery Times Objectives (RTO) e Recovery Point Objectives (RPO) para a função são incorporados nos planos de continuidade.

f. Os planos de continuidade são avaliados e testados.

i. Os resultados dos testes e/ou ativação do Plano de Continuidade são comparados aos objetivos de recuperação, e os planos são adequadamente melhorados.

j. Os Planos de Continuidade são revisados e atualizados periodicamente.

k. Os recursos restaurados são configurados adequadamente e as informações de inventário são atualizadas após a execução dos Planos de Continuidade.

IR-5: Atividades de Gerenciamento

a. Práticas documentadas são seguidas para resposta de eventos e incidentes de segurança cibernética, bem como a continuidade das atividades operacionais.

b. As partes interessadas para resposta de eventos e incidentes de segurança cibernética, bem como a continuidade das atividades operacionais, são identificadas e envolvidas.

d. Padrões e/ou diretrizes foram identificados para subsidiar a resposta a eventos e incidentes de cibersegurança, bem como a continuidade das atividades operacionais.

e -Resposta a eventos e incidentes de segurança cibernética, bem como a continuidade das atividades operacionais, são orientados por políticas documentadas ou outras diretrizes organizacionais.

f. Resposta a eventos e incidentes de segurança cibernética, bem como a continuidade das políticas de operações, incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

g. Resposta a eventos e incidentes de segurança cibernética, bem como a continuidade das atividades operacionais, são revisados periodicamente para garantir a conformidade com as políticas.

h. Responsabilidade e autoridade para o desempenho da resposta de eventos e incidentes de segurança cibernética, bem como a continuidade das atividades operacionais, são atribuídas às pessoas.

i. O pessoal que trata a resposta a eventos e incidentes de segurança cibernética, bem

como a continuidade das atividades operacionais, possuem as habilidades e os conhecimentos necessários para executar suas responsabilidades atribuídas.

GERENCIAMENTO DE CADEIA DE SUPRIMENTOS E DEPENDÊNCIAS EXTERNAS (EDM)

EDM-1: Identificar Dependências

a. Importantes dependências externas e de fornecedores de TI e TO (ou seja, partes externas das quais depende a entrega da função, incluindo parceiros operacionais) são identificadas pelo menos de maneira ad hoc.

b. Dependências importantes do cliente (ou seja, partes externas que dependem da entrega da função, incluindo parceiros operacionais) são identificadas pelo menos de maneira ad hoc.

c. Dependências externas e de fornecedores são identificadas de acordo com critérios estabelecidos.

d. Dependências do cliente são identificadas de acordo com critérios estabelecidos.

e. Fonte única e outras dependências essenciais são identificadas.

f. Dependências são priorizadas.

g. Priorização e identificação de dependência são baseadas nos critérios de risco da função ou organização (RM-1c).

EDM-2: Gerenciar Risco de Dependência

a. Riscos significativos de segurança cibernética, devido a fornecedores e outras dependências, são identificados e abordados, pelo menos de forma ad hoc.

j. Os riscos de segurança cibernética, devido a dependências externas, são gerenciados de acordo com os critérios e processos de gerenciamento de risco da organização.

n. As fontes de informação são monitoradas para identificar e evitar ameaças na cadeia de suprimentos (por exemplo, peças falsificadas, software e serviços).

EDM-3: Atividades de Gerenciamento

f. As políticas de gerenciamento de risco de dependência incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

GERENCIAMENTO DA FORÇA DE TRABALHO (WM)

WM-1: Atribuir Responsabilidades de Segurança Cibernética

a. As responsabilidades de segurança cibernética para a função são identificadas, pelo menos de maneira ad hoc.

b. As responsabilidades de segurança cibernética são atribuídas a pessoas específicas, pelo menos de maneira ad hoc.

c. As responsabilidades de segurança cibernética são atribuídas a funções específicas, incluindo provedores de serviços externos.

d. As responsabilidades de segurança cibernética são documentadas (por exemplo: nas descrições de posição).

e. As responsabilidades de segurança cibernética e os requisitos de trabalho são revisados e atualizados conforme apropriado.

f. As responsabilidades de segurança cibernética estão incluídas nos critérios de avaliação de desempenho do trabalho.

g. As responsabilidades de segurança cibernética atribuídas são gerenciadas para garantir a adequação e a redundância da cobertura.

WM-2: Controlar o Ciclo de Vida da Força de Trabalho

a. A investigação pessoal (por exemplo: verificação de antecedentes, testes de drogas) é realizada, pelo menos de maneira ad hoc, na contratação de posições que tenham acesso aos ativos necessários para a entrega da função.

b. Os procedimentos de rescisão de pessoal tratam da segurança cibernética, pelo menos de maneira ad hoc.

c. A investigação pessoal é executada em uma frequência definida pela organização para posições que têm acesso aos ativos necessários para a entrega da função.

d. Os procedimentos de transferência de pessoal abordam a segurança cibernética.

e. As designações de risco são atribuídas a todas as posições que têm acesso aos ativos necessários para a entrega da função.

f. A investigação pessoal é realizada para todas as posições (incluindo funcionários, fornecedores e contratados) em um nível compatível com a designação de risco de posição.

g. O planejamento de sucessão é executado para o pessoal com base na designação de risco.

h. Um processo formal de prestação de contas que inclui ações disciplinares é implementado para o pessoal que não cumprir as políticas e procedimentos de segurança estabelecidos.

WM-3: Desenvolver a Força de Trabalho de Segurança Cibernética

a. O treinamento em segurança cibernética é disponibilizado, pelo menos de maneira ad hoc, a funcionários com responsabilidades de segurança cibernética.

b. Os conhecimentos, competências e lacunas de capacidade em segurança cibernética são identificados.

c. As lacunas identificadas são abordadas através de recrutamento e/ou treinamento.

d. O treinamento em segurança cibernética é fornecido como um pré-requisito para a concessão de acesso a ativos que suportam a entrega da função (por exemplo: novo treinamento de pessoal, treinamento em transferência de pessoal).

g. Os programas de treinamento estão alinhados para apoiar os objetivos de gerenciamento da força de trabalho de segurança cibernética.

h. A eficácia dos programas de treinamento é avaliada em uma frequência definida pela organização e as melhorias são feitas conforme apropriado.

i. Os programas de treinamento incluem educação continuada e oportunidades de desenvolvimento profissional para o pessoal com responsabilidades significativas de segurança cibernética.

WM-4: Aumentar a Conscientização sobre Segurança Cibernética

a. Atividades de conscientização sobre segurança cibernética ocorrem, pelo menos de maneira ad hoc.

b. As partes interessadas, para as atividades de gerenciamento da força de trabalho de segurança cibernética, são identificadas e envolvidas.

WM-5: Gerenciamento de Atividades

f. As políticas de gerenciamento da força de trabalho de segurança cibernética incluem requisitos de conformidade para padrões e/ou diretrizes especificados.

GESTÃO DO PROGRAMA DE SEGURANÇA CIBERNÉTICA (CPM)

CPM-1: Estabelecer a Estratégia do Programa de Segurança Cibernética

c. A estratégia e as prioridades do programa de segurança cibernética são documentadas e alinhadas com os objetivos estratégicos da organização e risco à infraestrutura crítica.

g. A estratégia do programa de segurança cibernética é atualizada para refletir as mudanças nos negócios, as mudanças no ambiente operacional e as alterações no perfil de ameaças (TVM-1d).

CPM-2: Patrocinador do Programa de Segurança Cibernética

d. Financiamento adequado e outros recursos (ou seja, pessoas e ferramentas) são fornecidos para estabelecer e operar um programa de segurança cibernética alinhado com a estratégia do programa.

g. O desenvolvimento e manutenção de políticas de segurança cibernética é patrocinado.

k. O programa de segurança cibernética aborda e permite a obtenção da conformidade regulatória conforme apropriado.

CPM-3: Estabelecer e Manter a Arquitetura de Segurança Cibernética

a. Uma estratégia para isolar arquitetonicamente os sistemas de TI da organização dos sistemas TO, é implementada pelo menos de uma maneira ad hoc.

b. Uma arquitetura de segurança cibernética está em vigor para permitir segmentação, isolamento e outros requisitos que suportam a estratégia de segurança cibernética.

c. Segmentação e isolamento arquitetônico são mantidos de acordo com um plano documentado.

d. A arquitetura de segurança cibernética é atualizada em uma frequência definida pela organização para mantê-la atualizada.

CPM-4: Executar Desenvolvimento Seguro de Software

a. O software a ser implantado em ativos que são importantes para a entrega da função é desenvolvido usando práticas seguras de desenvolvimento de software.

CPM-5: Atividades de Gerenciamento

d. As atividades de gerenciamento do programa de segurança cibernética são guiadas por políticas documentadas ou outras diretrizes organizacionais.

PRÁTICAS ADICIONAIS

ABT-1: Práticas criadas pela ABRATE

a. Existe um documento descrevendo a filosofia de fluxo de dados na arquitetura de rede, pelo menos de maneira ad-hoc

b. Efetuar análise de risco com base no fluxo de dados, repositórios de dados, infraestrutura e conectividade

c. Os procedimentos de rede e outros requisitos regulatórios são conhecidos e respeitados

d. Os riscos ao negócio e impactos são identificados

e. Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos, de maneira informal

f. A tolerância ao risco organizacional é identificada

g. Os requisitos de detecção são definidos (por exemplo, não afetar a disponibilidade dos ativos)

h. As respostas aos eventos e incidentes de segurança cibernética são implementadas, pelo menos de maneira ad hoc

Apêndice C **– RESUMO DAS ETAPAS PARA USO DO FRAMEWORK**

Etapa 1: Priorizar e Definir o Escopo

Entradas	Atividades	Saídas
• Estratégia de gerenciamento de risco • Objetivos organizacionais e prioridades • Informações sobre ameaças	• Determinar onde será aplicado o Framework para avaliar e potencialmente guiar a melhoria dos recursos de segurança cibernética da organização	• Escopo de uso do framework

Etapa 2: Orientar

Entradas	Atividades	Saídas
• Escopo de uso do framework • Estratégia de gerenciamento de risco	• Identificar os sistemas e ativos dentro do escopo (por exemplo, pessoas, informações, tecnologia e instalações) e as referências normativas e informativas apropriadas (por exemplo, padrões, ferramentas, métodos e diretrizes de segurança cibernética e de riscos)	• Sistemas e ativos dentro do escopo • Requisitos de escopo (ou seja, regulatório, empresarial, organizacional) • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • Método de avaliação

Etapa 3: Criar um Perfil Atual

Entradas	Atividades	Saídas
• Sistemas e ativos dentro do escopo • Requisitos regulatórios de escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo • Método de avaliação	• Identificar a situação de segurança cibernética e gerenciamento de riscos da Organização	• Perfil atual

Etapa 4: Realizar uma avaliação de riscos

Entradas	Atividades	Saídas
• Escopo de uso do Framework • Estratégia de Gerenciamento de Risco • Abordagem de avaliação de risco definida pela organização • Requisitos regulamentares no escopo • Padrões, ferramentas, métodos e diretrizes de segurança cibernética e gerenciamento de risco no escopo	• Realizar avaliação de risco para o escopo da organização	• Relatório de avaliação de risco

Etapa 5: Criar um Perfil Alvo

Entradas	Atividades	Saídas
• Perfil atual • Objetivos organizacionais • Estratégia de gerenciamento de riscos • Relatório de avaliação de riscos	• Identificar metas que mitigarão o risco de acordo com seus objetivos	• Perfil Alvo

Etapa 6: Determinar, Analisar e Priorizar Lacunas

Entradas	Atividades	Saídas
• Perfil Atual • Perfil Alvo • Objetivos Organizacionais • Impacto para Infraestrutura Crítica • Lacunas e Potenciais Consequências • Restrições Organizacionais • Estratégia de Gerenciamento de Risco • Relatórios de Avaliação de Risco	• Análisar as lacunas entre o Perfil Atual e o Perfil Alvo no contexto de organização • Avaliar potenciais consequências advindas das lacunas • Determinar quais lacunas precisam de atenção • Identificar ações para endereçar as lacunas • Realizar análise de custo-benefício • Priorizar ações (Custo-benefício e Consequências) • Planejar a implementação de ações	• Lacunas priorizadas e potenciais consequências • Plano de implementação priorizado

Etapa 7: Executar o Plano de Ação

Entradas	Atividades	Saídas
• Plano de implementação priorizado	• Implementar ações por prioridade • Acompanhar o progresso em relação ao plano • Monitorar e avaliar os principais riscos, indicadores de desempenho e métricas • Relatório de Progresso	• Dados de acompanhamento do plano • Novas medidas de segurança implementadas

Apêndice D **– AGRADECIMENTOS**

Associação das Empresas Transmissoras de Energia Elétrica – ABRATE

Mário Miranda

Presidente da ABRATE

Coordenador da Força Tarefa de Segurança Cibernética ABRATE

Marcos Romeu Benedetti

ELETROSUL

Relator da Força Tarefa de Segurança Cibernética ABRATE

Luis Gustavo Coelho

ELETROSUL

Membros da Força Tarefa de Segurança Cibernética ABRATE (em ordem alfabética)

Alan Lara Soares STATEGRID	Erick Valleta STATEGRID	Marcelo Defacio Leal CTEEP
Alberto Wagner Collavizza CELEO REDES	Felipe Tatsch CEEE	Maria Cristina G. de Carvalho FURNAS
Alessandro Santana Moura CELG	Fernando Eduardo Covatti CEEE	Murilo Mascarenhas Menezes ELETRONORTE
Alexandre A. P. de Oliveira CHESF	Gabriella Gomide CELEO REDES	Nelio Kubo COPEL
Allyson Felipe da Silva Gomes TAESA	Henrique Soares de Almeida CELG	Pedro Paulo Gomes F. Garcia ITAIPU
Alvaro Tadeu de A. Pereira CHESF	João Silverio Dourado Pereira FURNAS	Ricardo Roscoe ELETRONORTE
Carlos Eduardo Bueno ITAIPU	José Newton F. Ferreira CEMIG	Roberto Sebastião J. Santos CEMIG
Claudio Hermeling COPEL	Luis Gustavo Coelho ELETROSUL	Sandro Monteiro da Cruz TAESA

Demais Colaboradores (em ordem alfabética)

Antonio Fernando de Souza
ELETROSUL

Ariel Francisco Andreiu
CELEO REDES

Basílio Smaczilo
ELETROSUL

Celso Soares Pereira
ELETROSUL

Daniel Kolm
ELETROSUL

Diogo Guimarães Alves
FURNAS

Edson José Marcolin
COPEL

Eduardo Di
STATEGRID

Eduardo Polvani Campaner
ELETROSUL

Ilídio José Bonfin Coutinho
EQUATORIAL

João Felipe Salomon Palma
HUAWEI

Jorge Luiz Braga Junior
TAESA

Marcelo Ayres Branquinho
TISAFE

Márcio Severi
ARGO

Matheus Araujo
CTEEP

Oslwaldo Alves
RNP

Pablo Humeres Flores
ELETROSUL

Paulo H. da Rosa Benites
ITAIPU

Rodrigo Facio
RNP

Sérgio Rodrigo P. de Araújo
EQUATORIAL

Thays Uchôa de Moraes
ELETROSUL

Thiago Braga Branquinho
TISAFE

Vitor Donaduzzi
CEEE