Manual de Orientação sobre Exercícios de Cibersegurança

FGV

Presidente
Carlos Ivan Simonsen Leal

Diretor Executivo FGV Projetos
Luiz Carlos Guimarães Duque

Diretor Adjunto FGV Projetos
Irineu Rodrigues Frare

Equipe Técnica FGV
Sérgio Gustavo Silveira da Costa (Coordenador)
Guilherme Ramon Garcia Marques
Isabella de Figueiredo Lopes Bodanese
Lorena Jacobson Berzins

Consultor técnico
Wilson Mendes Lauria

Pesquisadores voluntários
Juliana Zaniboni de Assunção
José Gabriel de Melo Pires

Projeto Gráfico
Bárbara da Rosa Amorim
Luiz Fernando Antunes

Comando de Defesa Cibernética (ComDCiber)

General de Divisão Fernando José Soares da Cunha Mattos
Coordenador do Gabinete de Crise do EGC 5.0

Contra Almirante Francisco André Barros Conde
Diretor do EGC 5.0 (fase de planejamento)

Brigadeiro do Ar Márlio Concidera Estebanez
Diretor do EGC 5.0 (fase de execução)

Capitão de Mar e Guerra (T) Antônio Carlos Pereira Borge
Coordenador Executivo do EGC 5.0

Coronel FAB Luciano Martins Menna
Coordenador de Relações Internacionais do EGC 5.0

Coronel EB Wandelino Moreno Junior
Apoiador do EGC 5.0

Coronel EB Daniel Davi Ramos da Silva Alves
Adjunto do Coordenador Executivo do EGC 5.0

Tenente Coronel EB Jorge Frederico Vieira Campos Flores
Coordenador do Grupo de Estudo e do Setor Academia do EGC 5.0

Sobre a FGV
Instituição de caráter técnico-científico, educativo e filantrópico, criada em 20 de dezembro de 1944, como pessoa jurídica de direito privado, tem por finalidade atuar no âmbito das Ciências Sociais, particularmente Economia e Administração, bem como contribuir para a proteção ambiental e o desenvolvimento sustentável. Sede: Praia de Botafogo, 190, Rio de Janeiro - RJ, CEP 22253-900

Sumário

Apresentações

Fundação Getulio Vargas

Embora não seja um acontecimento inédito na história – os Grandes Descobrimentos também representaram a expansão do espaço para a realização de atividades econômicas – a Era da Informação marca a criação de um novo espaço de natureza, esta sim, inédita. O espaço cibernético (ou ciberespaço), em contraste com a terra, o mar e o ar, dissocia-se do meio físico, e suas ações seguem lógica e velocidade próprias.

Os espaços de valor econômico são palco de atividades de distintos atores – indivíduos, empresas, ONGs e governos – e distintas naturezas – legais ou ilegais, regulamentadas ou não regulamentadas, pacíficas ou beligerantes, etc.

O ciberespaço não foge à regra, sendo um lócus para atividades que representam mais frequentemente riscos à segurança interna (ações criminosas), mas que também oferecem riscos à defesa e segurança internacional dos países. Existe, ainda, um agravante: a fluidez de suas fronteiras e a despersonalização de seus atores.

Apenas uma fração dessas atividades mira os meios de interligação entre o espaço físico e o ciberespaço, tais como servidores, bandas largas, PCs, impressoras, celulares e torres de transmissão de sinal. A maior parte do ciberespaço tem como alvo as camadas sintática e cognitiva deste último. A primeira é representada por protocolos de rede, formatação dos dados, e regras gramaticais e lógicas que guiam a comunicação entre sistemas e dispositivos. A segunda envolve a compreensão humana e a interpretação da informação, ensejando, por exemplo, práticas de phishing e desinformação.

Nos últimos anos, consolidou-se na sociedade brasileira a consciência dos riscos associados às atividades que têm lugar no ciberespaço e do imperativo de mitigá-los, para a qual o Exercício Guardião Cibernético (EGC), maior inciativa dessa natureza do Hemisfério Sul, cumpre um papel importante.

A FGV, dentro de suas áreas de atuação, tem contribuído para esse esforço por meio de iniciativas de capacitação, oferecidas pela FGV Educação Executiva, do apoio ao fortalecimento do arcabouço regulatório, por parte da FGV Direito Rio, e da participação como entidade apoiadora do EGC, capitaneada pela FGV Projetos.

Para a quinta edição do Exercício (EGC 5.0), por sugestão do Comando de Defesa Cibernética do Exército Brasileiro, a FGV uniu-se ao esforços pela disseminação da importância do engajamento da sociedade em atividades de cibersegurança e dos meios para fazê-lo.

Assim, o Manual de Orientação sobre Exercícios de Cibersegurança, que tem como público-alvo prioritário empresas e ONGs de diversos setores, associações de empresas e órgãos públicos que dispõem de pouca informação e têm interesse em realizar exercícios dessa natureza, surge como um marco de uma nova fase de disseminação da mensagem do EGC por todas as camadas da sociedade brasileira.

Carlos Ivan Simonsen Leal
Presidente da Fundação Getulio Vargas

Apresentações

FGV Projetos

A FGV Projetos é a unidade de assessoria técnica da Fundação Getulio Vargas e tem como objetivo auxiliar organizações públicas, empresariais e do terceiro setor, no Brasil e no exterior, desenvolvendo projetos nas áreas de economia e finanças, gestão e administração, e políticas públicas.

Há mais de uma década, dentro de seus campos de expertise, tem atuado em projetos das Forças Armadas e contribuído, dessa forma, para os esforços do País no campo da Defesa e Segurança Internacional, tendo sido credenciada em 12/06/2023 como Empresa Estratégica de Defesa (EED) pelo Ministério da Defesa.

Foi com muita honra que recebemos do Comando de Defesa Cibernética do Exército Brasileiro o desafio de conceber uma publicação visando contribuir, no âmbito de nossa atuação como entidade apoiadora do Exercício Guardião Cibernético e tomando por base sua bem-sucedida experiência, para o maior engajamento da Sociedade em atividades de cibersegurança.

Após estudar o desafio, propusemos que tal publicação se voltasse, fundamentalmente, a três objetivos.

Primeiramente, alcançar uma ampla gama de organizações – empresas e ONGs de diversos setores, associações de empresas e órgãos públicos – com portes, características e objetivos distintos.

Em segundo lugar, considerando toda essa diversidade, fornecer elementos para a decisão sobre a realização e a concepção de um exercício de segurança cibernética.

Finalmente, indo além do incentivo à realização de exercícios de segurança cibernética, contribuir para a difusão da mentalidade/cultura de segurança cibernética no Brasil.

Assim, chegou-se à proposta de desenvolver o Manual de Orientação sobre Exercícios de Cibersegurança, voltado para organizações que dispõem de pouca informação e têm interesse em realizar exercícios próprios de cibersegurança, e capaz de subsidiar esforços de conscientização por parte de organizações com maior grau de informação sobre o tema.

Apesar da complexidade do tema, o Manual foi elaborado em linguagem clara e direta, e organizado de modo a oferecer ao leitor elementos sobre “por que fazer um exercício de cibersegurança”, “o que fazer em um exercício de cibersegurança ” e “como fazer um exercício de cibersegurança”.

Finalmente, o Manual traz informações sobre a adoção de medidas de higiene cibernética, amplamente estimulada no âmbito do Exercício Guardião Cibernético, prática de natureza distinta dos exercícios de cibersegurança, mas que assume substantiva relevância para a prevenção às ameaças cibernéticas.

Luiz Carlos Guimarães Duque
Diretor Executivo da FGV Projetos

Apresentações

Comando de Defesa Cibernética

No cenário atual de constantes evoluções tecnológicas e ameaças cibernéticas cada vez mais sofisticadas, o Brasil tem se posicionado de maneira proativa na defesa de seus interesses no espaço digital.

O Exército Brasileiro, como responsável pelo Setor Cibernético conforme estabelecido na Estratégia Nacional de Defesa, permanece vigilante e pronto para enfrentar os desafios do domínio cibernético, sempre a serviço da nação e em defesa dos interesses do povo brasileiro, posicionando o País como um líder emergente em segurança cibernética na América Latina, além de reconhecer a criticidade do domínio cibernético para a soberania e o desenvolvimento nacionais.

Como Comandante de Defesa Cibernética, tenho a honra de apresentar uma reflexão sobre a importância do Manual de Orientação sobre Exercícios de Cibersegurança, resultado tangível do Acordo de Cooperação nº 23–ComDCiber–003–2024, estabelecido entre o Comando de Defesa Cibernética (ComDCiber) e a Fundação Getúlio Vargas (FGV), demonstrando a sinergia vital entre as capacidades militares e a acadêmica.

O Manual de Orientação sobre Exercícios de Cibersegurança, em conjunto com iniciativas como o Exercício Guardião Cibernético (EGC), exemplifica o compromisso do Exército Brasileiro com a excelência em defesa cibernética. Ele demonstra como a colaboração entre instituições militares, acadêmicas e do setor privado pode produzir resultados concretos para fortalecer nossa postura de segurança nacional.

A experiência e os insights obtidos durante a realização do EGC 5.0 foram fundamentais para a elaboração deste manual abrangente e prático. Ele foi concebido com um propósito claro: democratizar o conhecimento essencial sobre exercícios de cibersegurança. Seu público-alvo prioritário inclui empresas, ONGs de diversos setores, associações empresariais e órgãos públicos que dispõem de pouca informação, mas têm interesse em avaliar a possibilidade de realizar exercícios de cibersegurança.

Este manual não apenas fortalece nossas capacidades internas de defesa cibernética, mas também serve como um recurso valioso para toda a sociedade brasileira. Ele aborda temas cruciais como a importância da cibersegurança, tipos de exercícios, planejamento, coordenação, preparação logística e técnica, e execução de simulações de ataques cibernéticos.

Conclamo todos os setores da sociedade brasileira a fazerem uso destes valiosos recursos. A segurança cibernética é uma responsabilidade compartilhada, e apenas através de um esforço conjunto poderemos construir um ambiente digital seguro, protegendo nossos cidadãos, nossa economia e nossa soberania nacional.

Em conclusão, este manual representa um passo significativo em nossa jornada para construir um Brasil mais seguro e resiliente no espaço cibernético. Ele é um testemunho do compromisso do Exército Brasileiro com a excelência na defesa cibernética e da importância das parcerias entre instituições militares, acadêmicas e do setor privado.

General de Divisão Alan Denilson Lima Costa
Comandante do ComDCiber (Comando de Defesa Cibernética do Exército)

1. Introdução

1.1 Cibersegurança

A medida em que a humanidade avança na era digital, cujo principal motor de transformação é a revolução cibernética iniciada no último século do milênio passado e exponencialmente acelerada nesse início do terceiro milênio, envolvendo a utilização de tecnologias digitais e da internet em quase todos os aspectos da vida humana, a segurança cibernética, ou cibersegurança, assumiu uma importância crucial.

Os seguintes aspectos, cujos impactos, em muitos casos, se fazem sentir de forma sobreposta, podem ser destacados: a proteção das infraestruturas críticas, a segurança e defesa nacional, a proteção de informações sensíveis, a garantia da privacidade dos usuários e o arcabouço regulatório.

Qualquer ameaça cibernética representa, em alguma dimensão, um risco de perda. Mas estes riscos assumem dimensões cruciais em setores como energia, transporte, saúde e finanças, cujas atividades são altamente interconectadas a sistemas computacionais e redes de dados. Eventuais colapsos nas atividades desses setores, denominados de infraestruturas críticas, ao se disseminarem para outros setores, causarão imensos prejuízos econômicos, sociais e humanos, podendo, no limite, desestabilizar organizações, comunidades e nações.

No plano da segurança e defesa nacional, à medida em que sistemas de inteligência, policiamento e armamento, entre outros, também se encontrem interconectados a sistemas computacionais e redes de dados, essa vulnerabilidade a ciberataques também se faz invariavelmente presente, com sua efetiva materialização causando, igualmente, imensos prejuízos aptos a, no limite, desestabilizar organizações, comunidades e nações.

O imenso volume de informações sensíveis, incluindo dados pessoais, financeiros e empresariais que são armazenados e transmitidos online, expõe usuários, sejam organizações ou indivíduos, à uma série de ciberameaças, tais como o ataque de hackers, a penetração de *malwares* e outras violações de segurança. Essas ciberameaças a informações sensíveis, além do potencial para acarretar perdas financeiras, ferem o direito dos indivíduos à privacidade e podem, em última instância, minar a confiança da sociedade em relação ao funcionamento das instituições.

Finalmente, o objetivo de assegurar ou mitigar ameaças à segurança cibernética encerra um grande desafio para os arcabouços legais e regulatórios nacionais, cuja adaptação à revolução cibernética torna-se crucial para ordenar e organizar as ações da sociedade na era digital.

Os esforços em prol da segurança cibernética envolvem um conjunto multifacetado de medidas de proteção contra ameaças cibernéticas, cabendo destacar as seguintes dimensões:

Conscientização: Criação de consciência e promoção de uma cultura de segurança cibernética dentro das organizações e entre os indivíduos. Envolve educar colaboradores, *stakeholders* e o público em geral sobre riscos de segurança cibernética, melhores práticas e as consequências de ataques cibernéticos. Aumentar a conscientização ajuda as pessoas a reconhecerem ameaças potenciais, entender seu papel na manutenção da segurança e adotar medidas proativas para mitigar riscos;

Prevenção: Implementação de medidas para prevenir ataques cibernéticos e acesso não autorizado a sistemas, redes e dados. Isso inclui a implantação de tecnologias de segurança, como firewalls, softwares antivírus, sistemas de detecção de intrusão e controles de acesso para bloquear ou deter invasores. A prevenção também envolve a implementação de políticas, procedimentos e práticas de segurança para minimizar vulnerabilidades e fortalecer as defesas contra ameaças cibernéticas;

Detecção: Capacidade de identificar e detectar ameaças cibernéticas e incidentes de segurança em tempo hábil. Essa dimensão envolve a implantação de ferramentas de monitoramento, análise de segurança e sistemas de detecção de intrusão para monitorar o tráfego de rede, logs do sistema e padrões de comportamento em busca de sinais de atividades suspeitas ou maliciosas. A detecção precoce permite que indivíduos e organizações respondam rapidamente a incidentes de segurança, minimizando seu impacto de ataques e prevenindo maiores danos;

Resposta e mitigação: Como lidar com incidentes de segurança e ataques cibernéticos quando eles ocorrem? Essa dimensão envolve o estabelecimento de planos, procedimentos e equipes de resposta a incidentes para responder efetivamente a violações de segurança, conter os danos e mitigar os impactos. Abrange atividades como isolar sistemas comprometidos, restaurar backups, notificar os *stakeholders* e implementar medidas de correção para evitar incidentes futuros;

Resiliência: A resiliência cibernética se traduz na segurança dos sistemas de informação e organizacional de forma a preservar a capacidade de manter a continuidade dos negócios em face a incidentes de segurança ou ataques cibernéticos. Envolve a implementação preventiva de medidas tais como redundâncias, mecanismos de *failover* e planos de recuperação de desastres. Se traduz, ainda, na capacidade de recuperação de sistemas, dados e operações após um incidente de segurança ou ataque cibernético ensejando um aprimoramento das defesas cibernéticas. Essa dimensão enfatiza a importância de ter estratégias robustas e rápidas para o backup e a recuperação de dados e sistemas, minimizando o tempo de inatividade;

Governança e conformidade: Estabelecimento de políticas, procedimentos e estruturas para ordenar as práticas de segurança cibernética e garantir a conformidade com os requisitos regulatórios e os padrões estabelecidos. Envolve o desenvolvimento de políticas de segurança cibernética, a realização de avaliações de risco e o estabelecimento de estruturas de governança para supervisionar iniciativas de segurança cibernética. Também inclui o cumprimento de leis, regulamentos e padrões relevantes relacionados à proteção de dados, privacidade e segurança cibernética; e

Colaboração e compartilhamento de informações: Colaboração entre organizações, agências governamentais e profissionais de segurança cibernética para lidar com ameaças cibernéticas de forma eficaz. Envolve o compartilhamento de inteligência sobre ameaças, melhores práticas e recursos para aprimorar os esforços coletivos de segurança cibernética.

1.2 Exercícios de Cibersegurança

Os exercícios de cibersegurança são atividades simuladas que podem ser realizadas em âmbito nacional, setorial ou das organizações para testar e/ou aprimorar a prontidão, as capacidades de resposta e a resiliência das medidas contra potenciais ameaças e ataques cibernéticos. Respondem, também, à dimensão de conscientização.

Os exercícios internacionais de cibersegurança envolvem a colaboração e coordenação entre vários países para enfrentar ameaças cibernéticas transnacionais e aprimorar a cooperação em segurança cibernética. Nesse sentido, promovem o compartilhamento de informações, a colaboração e a assistência mútua entre os países participantes para incrementar as capacidades coletivas de segurança cibernética e a resposta à incidentes cibernéticos com implicações globais. Como exemplo, cabe destacar o *Locked Shields*, organizado pelo Centro de Excelência de Defesa Cibernética Cooperativa da OTAN, reunindo equipes desta aliança militar e de países parceiros para simular cenários de defesa cibernética no sentido de testar capacidades de proteção das infraestruturas críticas em resposta à ataques cibernéticos sofisticados.

Já os exercícios nacionais de cibersegurança são iniciativas em grande escala, organizados pelos governos nacionais para avaliar e melhorar a postura de cibersegurança de todo o país. Os exercícios nacionais de segurança cibernética envolvem várias agências governamentais, setores de infraestrutura crítica, parceiros do setor privado e parceiros internacionais. Simulam ataques cibernéticos, incidentes e cenários para testar as capacidades de coordenação, comunicação e resposta de vários *stakeholders* na proteção da segurança nacional, infraestrutura crítica e informações confidenciais. Como exemplos podem ser destacados:

- **Cyber Storm (Estados Unidos):** Exercício nacional bienal de segurança cibernética coordenado pelo Departamento de Segurança Interna (DHS). Reúne governos federal, estaduais, locais, territoriais, parceiros internacionais e organizações do setor privado para simular ataques cibernéticos e testar capacidades de resposta; e

- **Guardião Cibernético (Brasil):** O maior exercício simulado de defesa cibernética do hemisfério sul, equiparado aos principais exercícios internacionais. Realizado anualmente, tem por objetivo criar um ambiente realista por meio do qual instituições públicas e privadas de diversos setores, tais como, elétrico, água, financeiro, nuclear e de telecomunicações, atuam para proteger suas infraestruturas críticas de ataques cibernéticos. Contribui, portanto, para a integração entre governo, setor privado e meio acadêmico, em prol do crescimento da resiliência cibernética em áreas de interesse da defesa nacional.

Embora os exercícios de segurança cibernética de amplitude internacional e nacional sejam mais divulgados, iniciativas dessa natureza são realizadas, também, no âmbito das organizações.

1.3 O Manual de Orientação sobre Exercícios de Cibersegurança

A iniciativa de elaborar o Manual de Orientação sobre Exercícios de Cibersegurança responde a sugestão do Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro no contexto do apoio à realização da quinta edição do Exercício Guardião Cibernético (EGC 5.0). Entende-se que o incentivo à realização de exercícios por organizações é uma forma do EGC potencializar suas metas de conscientização sobre a importância de fortalecer a capacidade nacional de fazer frente a ameaças cibernéticas.

Nesse contexto, o público-alvo prioritário do Manual são organizações – empresas e ONGs de diversos setores, associações de empresas e órgãos públicos – que dispõem de pouca informação e têm interesse em realizar exercícios próprios de cibersegurança. O Manual visa subsidiar essas organizações com elementos sobre "por que fazer", "o que fazer" e "como fazer".

Além de incentivar a realização de exercícios de cibersegurança, as informações contidas no Manual contribuirão para a difusão da mentalidade/cultura de cibersegurança nas organizações, podendo, nesse sentido, subsidiar ações de conscientização por parte de organizações com maior grau de informação sobre o tema.

A Figura 1.3.1 apresenta a estrutura do Manual.

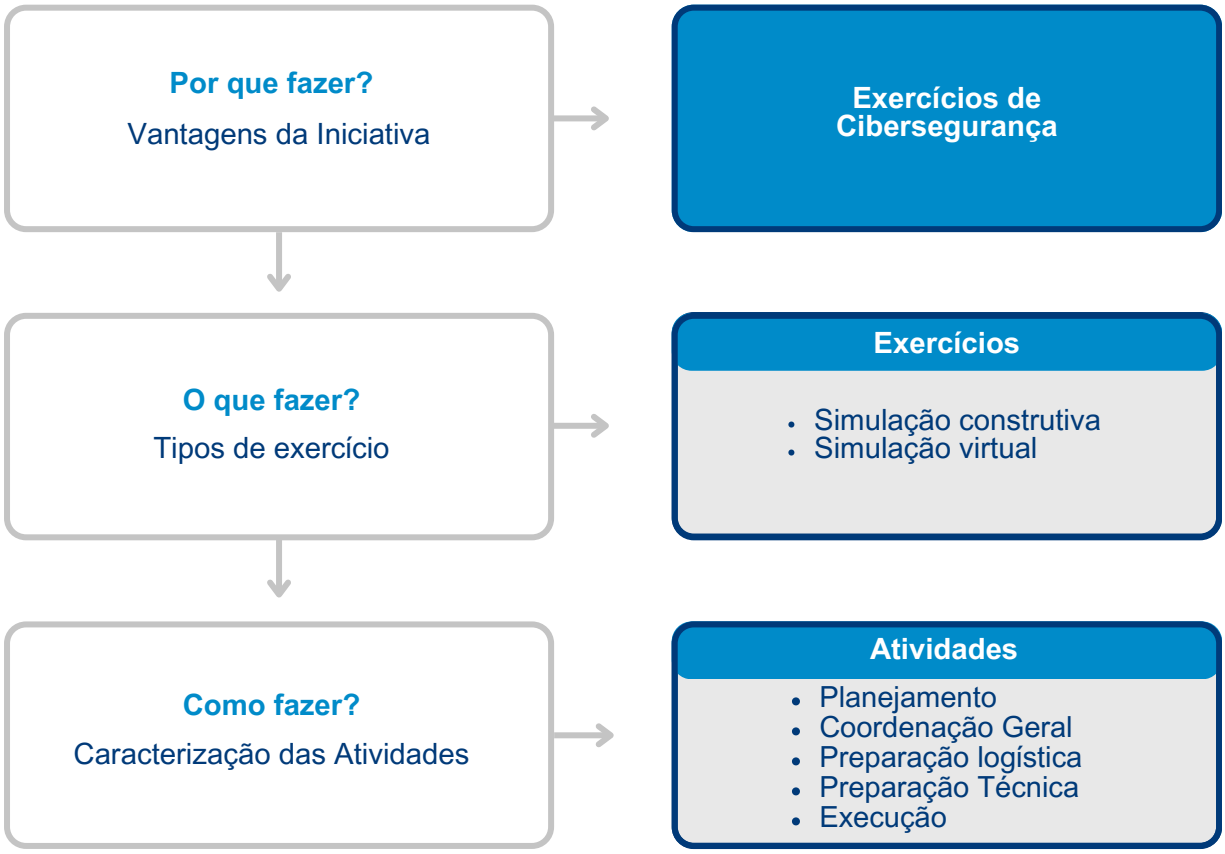


Figura 1.3. 1 Estrutura do Manual

Inicialmente, na **Seção 2 (“Por que fazer?”)**, o Manual apresenta vantagens dos exercícios enquanto ferramenta para o aprimoramento da cibersegurança em organizações.

Em seguida, na **Seção 3 (“O que fazer?”)**, o Manual caracteriza as duas modalidades tradicionais de exercícios de segurança cibernética: simulação construtiva e virtual.

Na **Seção 4 (Como fazer?)**, o Manual caracteriza e detalha as atividades consideradas essenciais no contexto dos exercícios de segurança cibernética: o planejamento, a Coordenação Geral, preparação logística, a preparação técnica e execução.

Embora com natureza distinta dos exercícios de cibersegurança, a adoção de medidas de higiene cibernética como prática regular assume relevância no contexto dos esforços das organizações para a prevenção às ameaças cibernéticas, sendo estimulada no âmbito do EGC. Nesse contexto o Manual apresenta em seu **Anexo 1** informações sobre esse tema.

No **Anexo 2** apresenta-se glossário dos principais termos técnicos presentes no Manual.

Finalmente, nos **Anexos 3 e 4**, apresentam-se indicações bibliográficas relevantes e informações sobre seu conteúdo.

2. Por que fazer?

Em essência, uma organização que executa uma operação ou uma função ou um negócio dependendo de informações, dados, redes ou sistemas de comunicações está operando no ciberespaço. Atualmente, as operações do ciberespaço são fundamentais para o sucesso e credibilidade de qualquer organização, seja ela pequena ou grande, pública ou privada.

No entanto, muitas organizações deixam de testar suas capacidades cibernéticas e processos de negócios para avaliar sua prontidão e conformidade com os requisitos normativos, identificar vulnerabilidades, treinar colaboradores e testar planos de resposta a incidentes de forma a se precaver contra ameaças cibernéticas e ter capacidade de resposta em caso da ocorrência de incidentes.

A implementação de um exercício de cibersegurança enseja a consecução desses objetivos a medida que:

- Permite colocar todas as áreas e *stakeholders* à par da importância desta prática constante;
- Examina o quão preparada uma organização está, e suas capacidades de resposta em um ambiente controlado;
- Valida e identifica brechas nas políticas, planos e procedimentos;
- Estabelece e melhora parcerias para aprimorar a conscientização sobre o compartilhamento de informações confidenciais;
- Expõe tomadores de decisão a situações de crise;
- Durante a fase de planejamento permite testar vários times de cenários de crises, procedimentos conceituais e técnicos e estratégias de mitigação;
- Avalia as capacidades no nível individual dos participantes das organizações;
- Permite a prática de coordenação de resposta de incidentes;
- Direciona melhorias operacionais de forma efetiva; e
- Aumenta a conscientização sobre ataques cibernéticos.

E, o que é muito importante, por ser realizado por meio de simulações em ambientes controlados, apresenta baixo custo e baixo risco.

3. O que fazer?

Esta seção caracteriza as duas modalidades tradicionais de exercícios de cibersegurança: simulação construtiva e virtual.

Apresenta-se na Figura 3.1 um resumo esquemático dos itens apresentados a seguir.

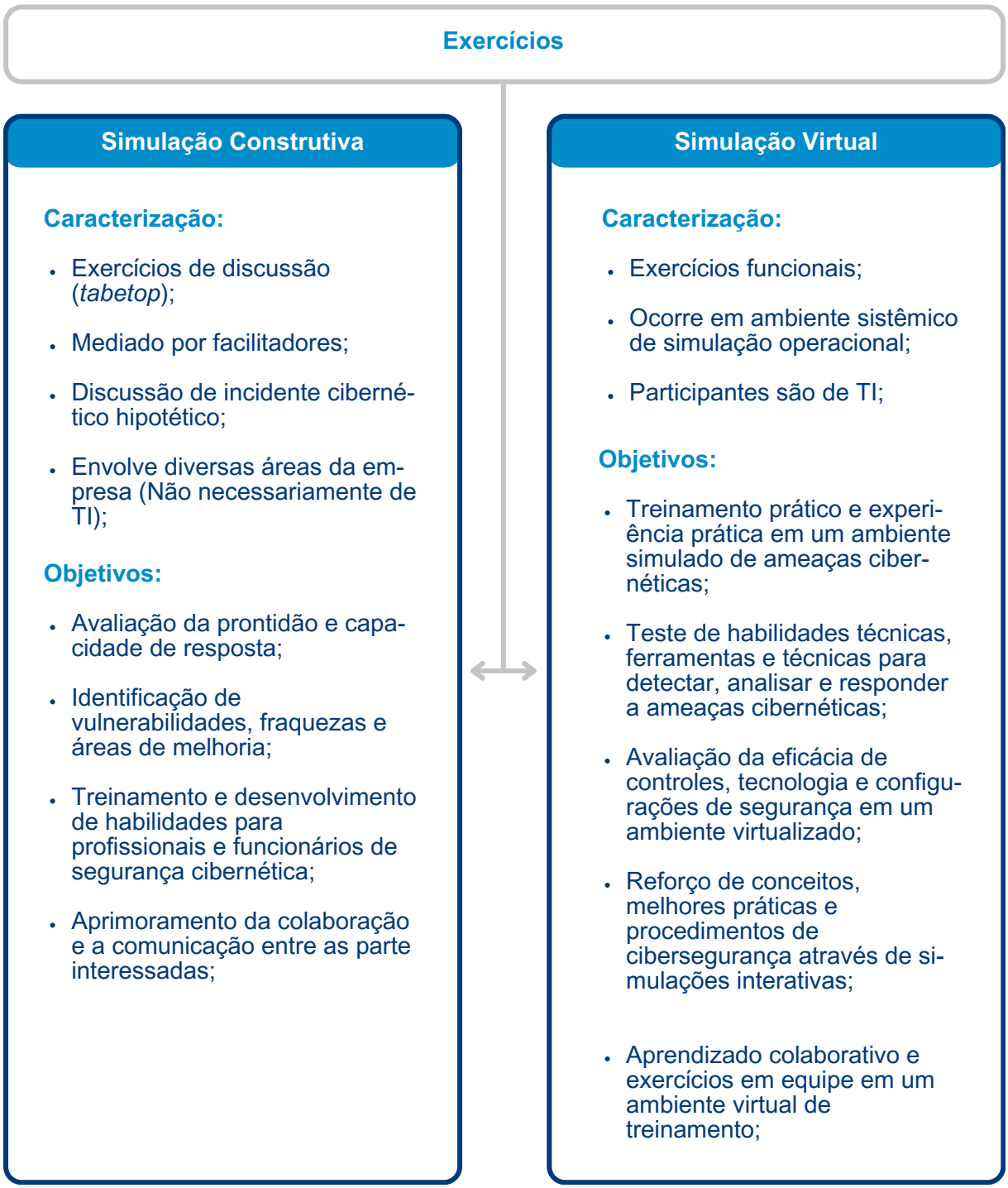


Figura 3.1

3.1 Simulações Construtiva e Virtual

A estruturação das simulações desponta como um eixo central na condução dos exercícios de cibersegurança, com todas as demais áreas de trabalho gravitando em sua órbita no sentido de criar as condições propícias para que os participantes possam usufruir das melhores experiências durante o exercício.

É crucial, portanto, que as simulações sejam rigorosamente planejadas de modo a testar e avaliar as habilidades de resiliência institucional, bem como promover o desenvolvimento de capacidades essenciais que vão desde a identificação de vulnerabilidades cibernéticas até a aplicação de procedimentos de caráter emergencial, em plena consonância com o conjunto de metas e objetivos estabelecidos no âmbito do exercício.

Nesse sentido, as simulações podem ser desenhadas para, dentre outros propósitos:

- Avaliar a cooperação técnica e operacional durante crises cibernéticas, garantindo fluxos contínuos de informações críticas entre as áreas da organização;
- Treinar a área responsável para atuar durante a crise, gerenciando o incidente crítico em suas múltiplas frentes – desde o enfrentamento direto ao ataque, minimizando seus prejuízos tangíveis e intangíveis, até a mobilização e distribuição de recursos críticos e organização logística, o que inclui desde protocolos para a evacuação e abrigo até o acesso a serviços essenciais, quando aplicável;
- Aprimorar o nível de consciência situacional;
- Testar a coordenação operacional de relações públicas; e
- Testar a implementação de processos planejados de recuperação pós-incidente, estabelecendo prioridades de retorno e avaliações de impacto.

Tais simulações não são apenas exercícios, mas uma oportunidade valiosa de promover capacidades de resiliência e prontidão por parte das organizações, estreitando laços e estruturas de colaboração entre as suas áreas.

Em essência, as simulações podem ser configuradas em dois formatos distintos, cada qual com suas particularidades, assumindo níveis de complexidade variados em vista dos objetivos estabelecidos e da própria maturidade cibernética da organização.

Simulação Construtiva

Cria-se um ambiente simulado que reproduz elementos, o mais fielmente possível, ao ambiente real de uma organização. Durante esta fase, os participantes praticam e testam suas habilidades sem comprometer o dia a dia da organização. São exemplos de exercícios de simulação construtiva:

- **Resposta a incidentes:** Os participantes simulam incidentes de segurança, como uma violação de dados ou ataque de *malware*. Com isso, podem praticar processos como a identificação, classificação, contenção e recuperação, seguindo os procedimentos de resposta a incidentes previamente estabelecidos;

- **Treinamento em resposta a ataques de *phishing*:** Os participantes desenvolvem estratégias de resposta a ataques de *phishing* simulados, incluindo identificação, notificação e mitigação de possíveis danos;

- **Recuperação de desastres cibernéticos:** Os participantes atuam em simulações de incidentes graves, como ataques de *ransomware*, para testar procedimentos de recuperação de desastres cibernéticos e avaliar o tempo de recuperação;

- **Avaliação de políticas de segurança:** Os participantes podem rever e ajustar políticas de segurança da informação durante a simulação, incluindo a análise de seu impacto nas operações diárias; e

- **Identificação de vazamento de dados:** Os participantes simulam um vazamento de dados para treinar a equipe na identificação rápida, contenção e notificação de incidentes de segurança.

Simulação Virtual

Utiliza ferramentas virtuais para simular cenários de cibersegurança. Configura-se como um treinamento realista, adaptado aos objetivos individuais da organização, com os participantes desenvolvendo suas habilidades em resposta às simulações e situações específicas de ataques cibernéticos. São exemplos de exercícios de simulação virtual:

- **Configuração de *firewalls*:** Os participantes podem praticar a configuração de firewalls, explorando diferentes conjuntos de regras para permitir ou bloquear tráfego com base em políticas de segurança. Isso inclui a definição de regras específicas para aplicações, protocolos e endereços IP;
- **Detecção de intrusão:** Os participantes podem configurar e ajustar sistemas de detecção de intrusão. Isso envolve a definição de assinaturas, análise de logs e resposta a alertas de segurança. A prática inclui a identificação de atividades suspeitas e a tomada de medidas adequadas;
- **Configuração de sistemas de detecção de *malwares*:** Os participantes podem simular a configuração e otimização de sistemas de detecção de *malwares*, explorando diferentes configurações para aprimorar a eficácia da detecção;
- **Análise de tráfego de rede suspeito:** Os participantes atuam na análise de padrões de tráfego de rede, visando identificar atividades suspeitas; e
- **Testes de resiliência de redes virtuais privadas (VPNs):** Os participantes configuram testes de redes VPN para garantir a segurança e a eficiência da comunicação remota, simulando diferentes cenários de conectividade e avaliando a resiliência de sua infraestrutura.

Pode-se dizer que a simulação construtiva prioriza o treinamento de processos, ao passo que a simulação virtual prioriza o treinamento de procedimentos. O critério de escolha entre estes formatos deverá basear-se nas necessidades e objetivos institucionais de cada organização, assim como nas capacidades, condições e recursos disponíveis para a realização do exercício. Se a organização considerar desejável, poderá ainda realizar as duas simulações de forma simultânea – neste caso, é imperativo ter clareza no que se refere aos objetivos propostos e às ferramentas necessárias para a execução eficaz de cada uma delas.

A seguir, apresentam-se informações complementares sobre os dois formatos de simulação.

Simulação Construtiva

As simulações construtivas normalmente envolvem exercícios *tabletop*, a partir de discussões mediadas por facilitadores (por exemplo, simular um ataque de *ransomware* na rede de uma instituição financeira). De forma geral, solicita-se aos participantes para discutirem um incidente cibernético hipotético e apresentarem abordagens para remedia-lo ou recuperar o dano, com referência a processos e procedimentos organizacionais existentes. Esse formato permite discussões profundas e produz decisões que não foram vivenciadas até então dentro da organização.

Essas simulações são conduzidas usando cenários hipotéticos, onde os participantes discutem e analisam suas respostas, decisões e ações sem a simulação de ataques cibernéticos ou modificação de sistemas reais.

Os exercícios de simulação construtiva ensejam:

- Avaliação da prontidão e capacidade de resposta;
- Identificação de vulnerabilidades, fraquezas e áreas de melhoria;
- Treinamento e desenvolvimento de habilidades para profissionais e funcionários de segurança cibernética;
- Teste de planos, procedimentos e mecanismos de coordenação de resposta a incidentes;
- Aprimoramento da colaboração e a comunicação entre os *stakeholders*; e
- Exercitar as capacidades não tecnológicas, ou seja, das áreas jurídica, da proteção de dados (DPO), de comunicação, de marketing etc.

Simulação Virtual

As simulações virtuais, que utilizam ambientes virtuais tais como cyber ranges, normalmente envolvem exercícios funcionais: os participantes assumem diferentes papéis, como atacantes (*red team*) e defensores (*blue team*), para trabalhar em vários cenários de ataque cibernético (por exemplo, a avaliação dos recursos de resposta e detecção: detecção de ativos computacionais da organização, máquinas com sistemas operacionais desatualizados ou descontinuados). Ocorrem em ambiente computacional virtual em que os participantes têm papéis e funções num plano de resposta a incidentes cibernéticos. Este formato permite à organização testar seus processos quando estiverem respondendo a incidentes cibernéticos.

Envolvem o uso de simulações computacionais para replicar cenários e ambientes de ataques cibernéticos em um ambiente virtual. Aproveitam a tecnologia para criar cenários realistas de ataques cibernéticos e permitem que os participantes interajam com sistemas, redes e ambientes para praticar e treinar em um cenário simulado de ameaças cibernéticas.

Nas simulações virtuais, os participantes têm papéis e funções num plano de resposta a incidentes cibernéticos. Este formato permite à organização testar seus equipamentos, hardware, software e outras habilidade quando estiverem respondendo à incidentes cibernéticos.

As simulações virtuais utilizam plataformas especializadas de treinamento em cibersegurança que fornecem ambientes virtualizados, infraestruturas de rede e ferramentas para simular ataques cibernéticos, incidentes e cenários. Nesse sentido, os participantes interagem com o ambiente virtual usando ferramentas e interfaces simuladas, a partir das quais realizam exercícios práticos em resposta a ameaças cibernéticas simuladas em tempo real. As simulações virtuais podem incluir cenários como invasões de rede, infecções por *malware*, violações de dados e ataques de negação de serviço como, por exemplo, o uso de uma plataforma de alcance cibernético para simular um ataque distribuído de negação de serviço (DDoS), induzindo os participantes a praticarem a mitigação do ataque usando ferramentas e técnicas de segurança de rede, ou mesmo uma simulação virtual envolvendo um surto de *malware*, permitindo que os participantes possam treinar equipes de resposta a incidentes sobre procedimentos de análise, contenção e erradicação de *malwares*.

Os exercícios de simulação virtual ensejam:

- Treinamento em um ambiente simulado de ameaças cibernéticas;
- Teste de habilidades técnicas, ferramentas e técnicas para detectar, analisar e responder a ameaças cibernéticas;
- Avaliação da eficácia de controles, tecnologias e configurações de segurança em um ambiente virtualizado;
- Reforço de conceitos, melhores práticas e procedimentos de cibersegurança através de simulações interativas; e
- Aprendizado colaborativo e exercícios em equipe em um ambiente virtual de treinamento.

4. Como fazer?

Esta seção caracteriza e detalha as atividades consideradas essenciais no contexto dos exercícios de segurança cibernética: o planejamento, a coordenação geral, a preparação logística, a preparação técnica e a execução.

O escopo e amplitude de tais atividades variam em complexidade de acordo com as particularidades da organização e o tamanho e dimensão propostos para o exercício.

Nesse sentido, cabe ressaltar que as informações apresentadas no presente Manual devem ser tomadas como um quadro de referência geral, cabendo-lhes a flexibilidade e adaptabilidade necessárias ao contexto em que forem aplicadas por cada organização.

Apresenta-se na Figura 4.1 um resumo esquemático dos itens apresentados a seguir, que representa a Estrutura Analítica de Projeto (EAP) para um exercício de cibersegurança, considerada no presente Manual.

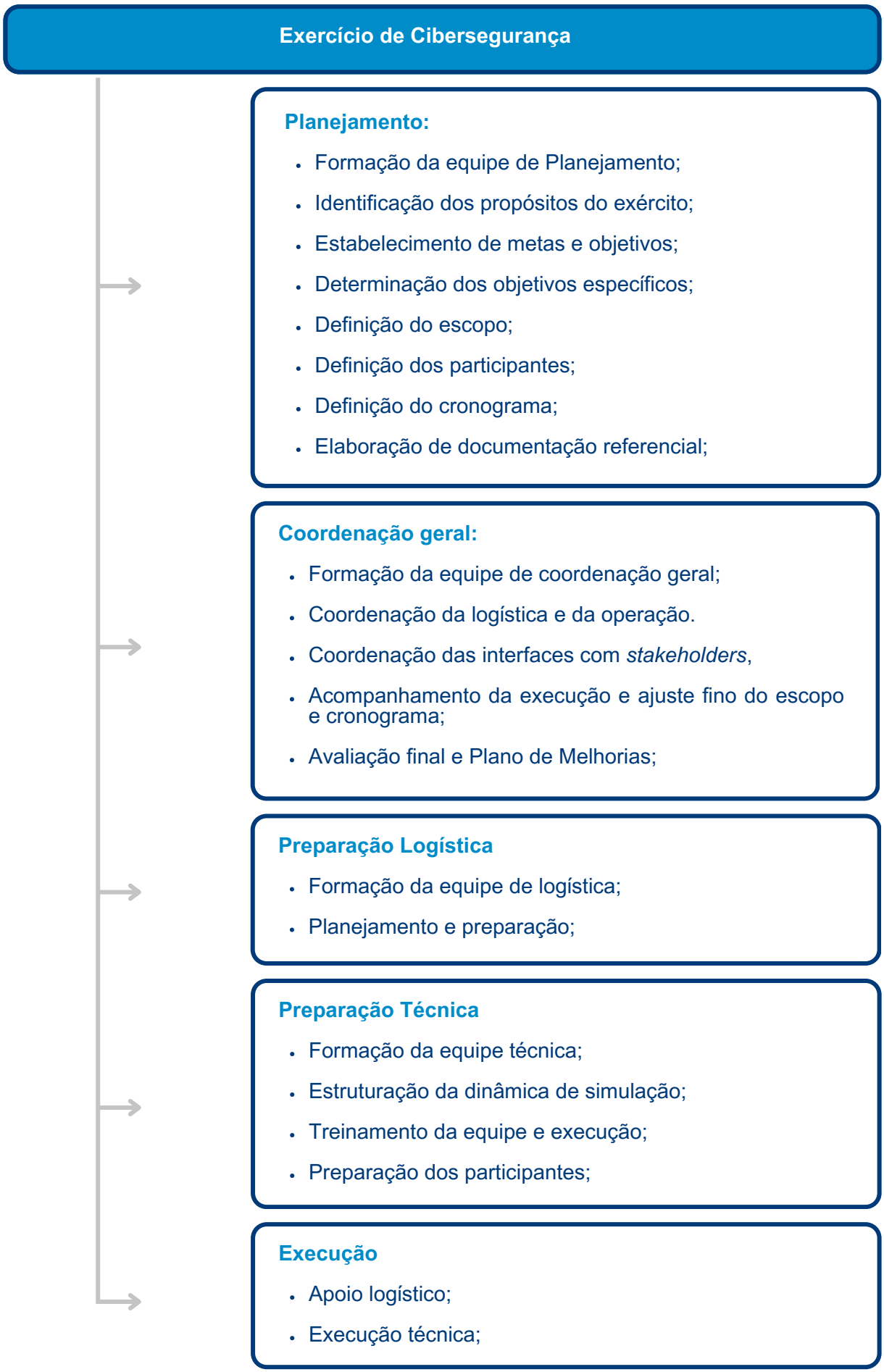

Exercício de Cibersegurança
Planejamento:
Formação da equipe de Planejamento;
Identificação dos propósitos do exército;
Estabelecimento de metas e objetivos;
Determinação dos objetivos específicos;
Definição do escopo;
Definição dos participantes;
Definição do cronograma;
Elaboração de documentação referencial;
Coordenação geral:
Formação da equipe de coordenação geral;
Coordenação da logística e da operação.
Coordenação das interfaces com stakeholders,
Acompanhamento da execução e ajuste fino do escopo e cronograma;
Avaliação final e Plano de Melhorias;
Preparação Logística
Formação da equipe de logística;
Planejamento e preparação;
Preparação Técnica
Formação da equipe técnica;
Estruturação da dinâmica de simulação;
Treinamento da equipe e execução;
Preparação dos participantes;
Execução
Apoio logístico;
Execução técnica;

Figura 4.1

4.1 Planejamento

O sucesso de um exercício de cibersegurança começa antes de sua efetiva execução. A gestão de projetos, enquanto metodologia voltada para a coordenação de atividades com o objetivo de concretizar as expectativas dos *stakeholders* de um dado projeto, destaca a importância fundamental da etapa de planejamento como forma de assegurar a execução adequada das atividades previstas e a tomada de decisão em resposta a eventos não previstos.

O planejamento exige níveis intensivos de coordenação entre os colaboradores e áreas envolvidos, em um esforço estruturado e integrado voltado a garantir a realização de um exercício com representação precisa da realidade da organização, em seus desafios e ameaças crescentes e constantes.

No contexto aplicado aos exercícios de cibersegurança, o planejamento envolve as seguintes atividades:

1) Formação da equipe de planejamento;

2) Identificação dos propósitos do exercício;

3) Estabelecimento de metas e objetivos;

4) Determinação dos objetivos específicos;

5) Definição do escopo;

6) Definição dos participantes;

7) Definição do cronograma; e

8) Elaboração de documentação referencial.

1) Formação de equipe de planejamento

Inicialmente, a equipe de planejamento deve ser formada por um núcleo restrito de colaboradores da organização aptos a dar o pontapé inicial de validar com a liderança da organização as razões e justificativas para a realização do exercício. Conforme a definição dos propósitos, escopo, metas e objetivos específicos for avançando, estarão disponíveis mais elemento para a avaliação da necessidade de robustecer a equipe, o que pode envolver a alocação de outros colaboradores e até a contratação de pessoas.

De toda forma, a equipe de planejamento deve abranger, no mínimo, as seguintes funções:

- **Coordenador geral:** Têm a responsabilidade de planejar os diversos aspectos logísticos, técnicos e operacionais associados à execução do exercício. Deve possuir um entendimento holístico de todas as dimensões e etapas do exercício; e

- **Coordenadores de áreas:** Têm a responsabilidade de apoiar o coordenador do exercício no planejamento dos aspectos logísticos e técnicos associados à execução do exercício. É crucial ter, pelo menos, dois coordenadores especialistas: para a área logística e para área técnica, assegurando uma cobertura abrangente e eficaz das múltiplas atividades a serem empreendidas.

A critério da organização, o Coordenador geral pode acumular a função dos coordenadores de área (logístico e/ou técnico).

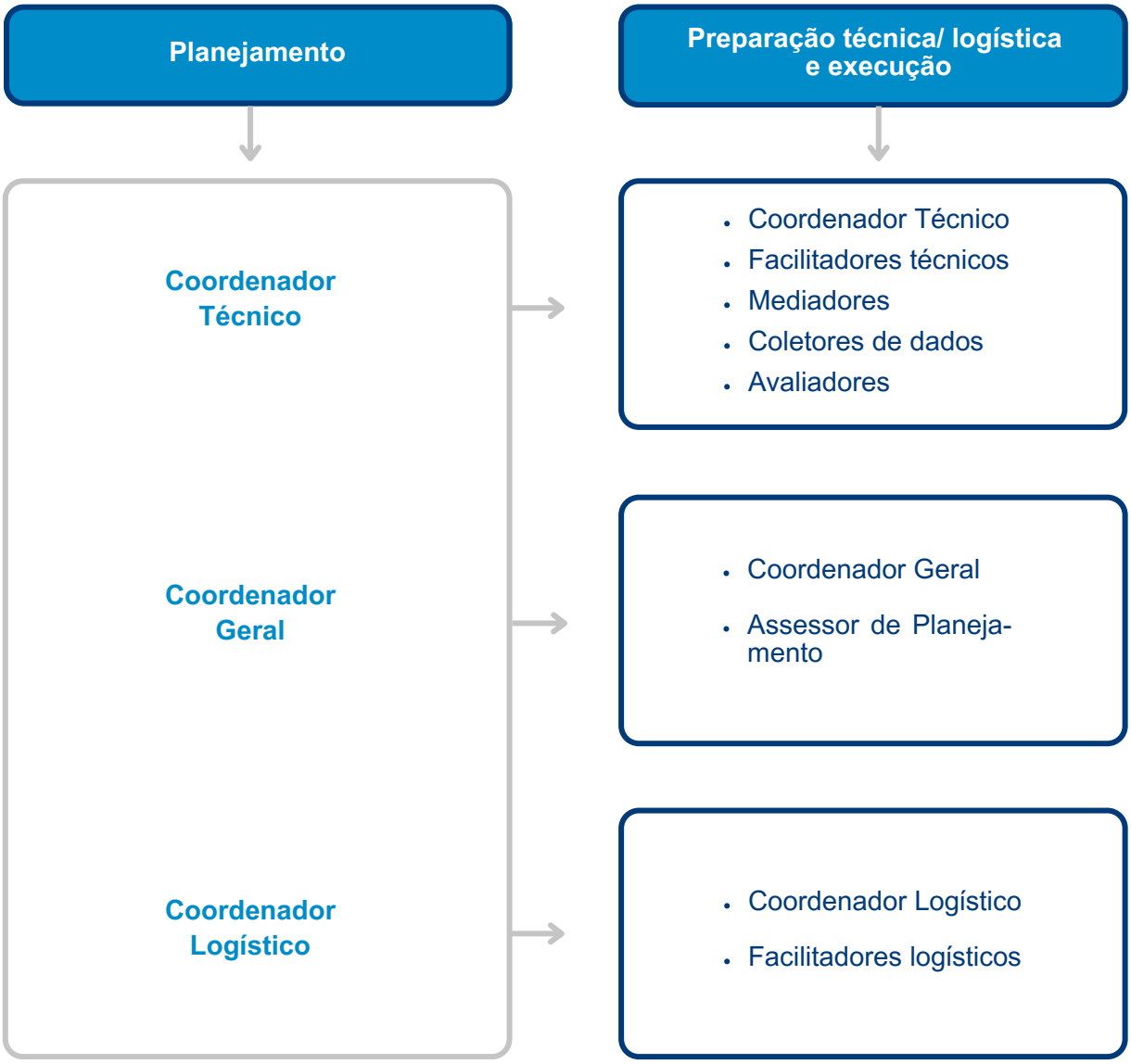
A equipe de planejamento também responde e representa toda a gama de *stakeholders*, incluindo as que não irão participar do exercício. Para um exercício que envolva múltiplas áreas da organização, pode ser relevante tê-las representadas no time de planejamento, ensejando uma amplitude maior de perspectivas e facilitando a comunicação com essas áreas

Tipicamente, os membros da equipe de planejamento são agentes de confiança e, idealmente, não devem ser participantes do exercício. Caso os recursos sejam limitados, os membros do time podem vir a ser os participantes, mas é importante ter o cuidado de não compartilhar com eles quaisquer informações confidenciais do exercício.

A equipe de planejamento também auxilia na produção e distribuição de materiais referenciais para o exercício.

É recomendável que se avalie cuidadosamente quem deve fazer parte do time e que seja uma quantidade gerenciável de pessoas. Baseado no objetivo do exercício, devem ser identificadas as áreas da organização que possam ceder colaboradores.

Conforme será visto nos itens seguintes, e ilustrado na Figura 4.1.1, assim que encerrada a etapa de planejamento propriamente dita, os integrantes da equipe do planejamento passarão a compor as equipes de coordenação geral, de coordenação logística e de coordenação técnica.



Independentemente do desdobramento e do crescimento da equipe, é imprescindível que o alinhamento com os elementos norteadores já estabelecidos seja preservado, cabendo-lhe zelar pelo cumprimento do propósito e objetivos estabelecidos para o exercício. Ademais, sua configuração deve ser aderente à estrutura organizacional da organização.

Figura 4.1.1
Coordenações do exercício de cibersegurança

2) Identificação dos propósitos do exercício

O ponto de partida para o planejamento de exercícios de cibersegurança é a identificação dos propósitos do exercício em consonância com as necessidades da organização.

O propósito do exercício é o farol que alinhará tanto expectativas como ações que devem ser realizadas. É a primeira pergunta que deve ser respondida pela organização no contexto do planejamento do exercício.

A título de exemplo, esses propósitos podem incluir, mas não se limitar, a:

- Identificar potenciais ameaças já estabelecidas ou emergentes;
- Identificar áreas específicas para a promoção e o desenvolvimento de capacidades de segurança cibernética;
- Promover o treinamento contínuo do seu corpo geral de funcionários;
- Realizar ajustes e atualizações em políticas e procedimentos técnicos e operacionais;
- Adequar seus procedimentos aos requisitos legislativos ou regulatórios vigentes; e
- Implementar e desenvolver uma equipe especializada de cibersegurança.

Importante destacar que o sucesso da execução de um exercício de cibersegurança depende fundamentalmente do comprometimento da liderança organizacional no sentido de promover maior conscientização holística acerca das prioridades de cibersegurança no âmbito da organização.

3) Estabelecimento de metas e objetivos

O sucesso de um exercício de cibersegurança depende, indispensavelmente, da definição de metas e objetivos claros, ou seja, uma declaração geral capaz de descrever a intenção do resultado a ser alcançado, devendo ser definida a partir dos fatores que motivarão a realização do exercício em si. Em síntese, é a condição mais crítica para o sucesso do exercício.

A ausência de clareza em relação aos objetivos poderá acarretar complicações à formulação de um exercício com características apropriadas.

Nesse sentido, é fundamental que os objetivos estabelecidos sejam realistas e alinhados ao conjunto de necessidades e prioridades da organização.

4) Determinação dos objetivos específicos

Os objetivos específicos devem ser delineados considerando as particularidades e especificidades da organização, sobretudo no que se refere à sua atuação e seu planejamento, políticas e procedimentos internos. Podem abarcar, ainda, lições aprendidas de exercícios anteriores ou de análises de incidentes cibernéticos reais.

É fundamental que os objetivos específicos estabelecidos sejam materializáveis.

Exemplo

O objetivo como "aumentar a resiliência cibernética da equipe" pode ser desdobrado em objetivos específicos, como:

- Garantir que todos os sistemas, softwares e ferramentas utilizadas pela equipe estejam atualizados com os dispositivos de segurança mais recentes;
- Realizar avaliações regulares de vulnerabilidades e testes de penetração para identificar e mitigar possíveis brechas na segurança;
- Oferecer oportunidades de treinamento e certificação para a equipe a fim de aprimorar suas habilidades técnicas e de liderança; e
- Estabelecer canais de comunicação eficientes para garantir a rápida disseminação de informações relevantes durante incidentes cibernéticos.

É importante assinalar que o processo de formulação de objetivos específicos deve dialogar e estar ancorados nos seguintes elementos;

- Ações práticas ou atividades específicas a serem realizadas durante a realização do exercício;
- Processos que deverão ser acionados frente às ameaças e ao contexto de crise, viabilizando, assim, testar, explorar, avaliar, validar e revisar sua aplicação e desempenho – a exemplo de um plano de resposta a incidentes, de políticas, procedimentos e arranjos internos para a distribuição de responsabilidades ou mesmo de protocolos de ação e respostas especializadas; e
- O cenário hipotético (*storytelling*) que caracteriza o contexto geral do exercício, em suas simulações e atividades. Se o cenário hipotético não for realista, ou seja, aderente a realidade da organização, será mais difícil motivar os participantes e conduzi-los a atingir os objetivos traçados.

Dica

Casos práticos ajudam a ilustrar como um objetivo específico pode ser estruturado para abordar incidentes cibernéticos significativos, abrangendo ações práticas e o acionamento de processos dentro de um contexto hipotético. Por exemplo:

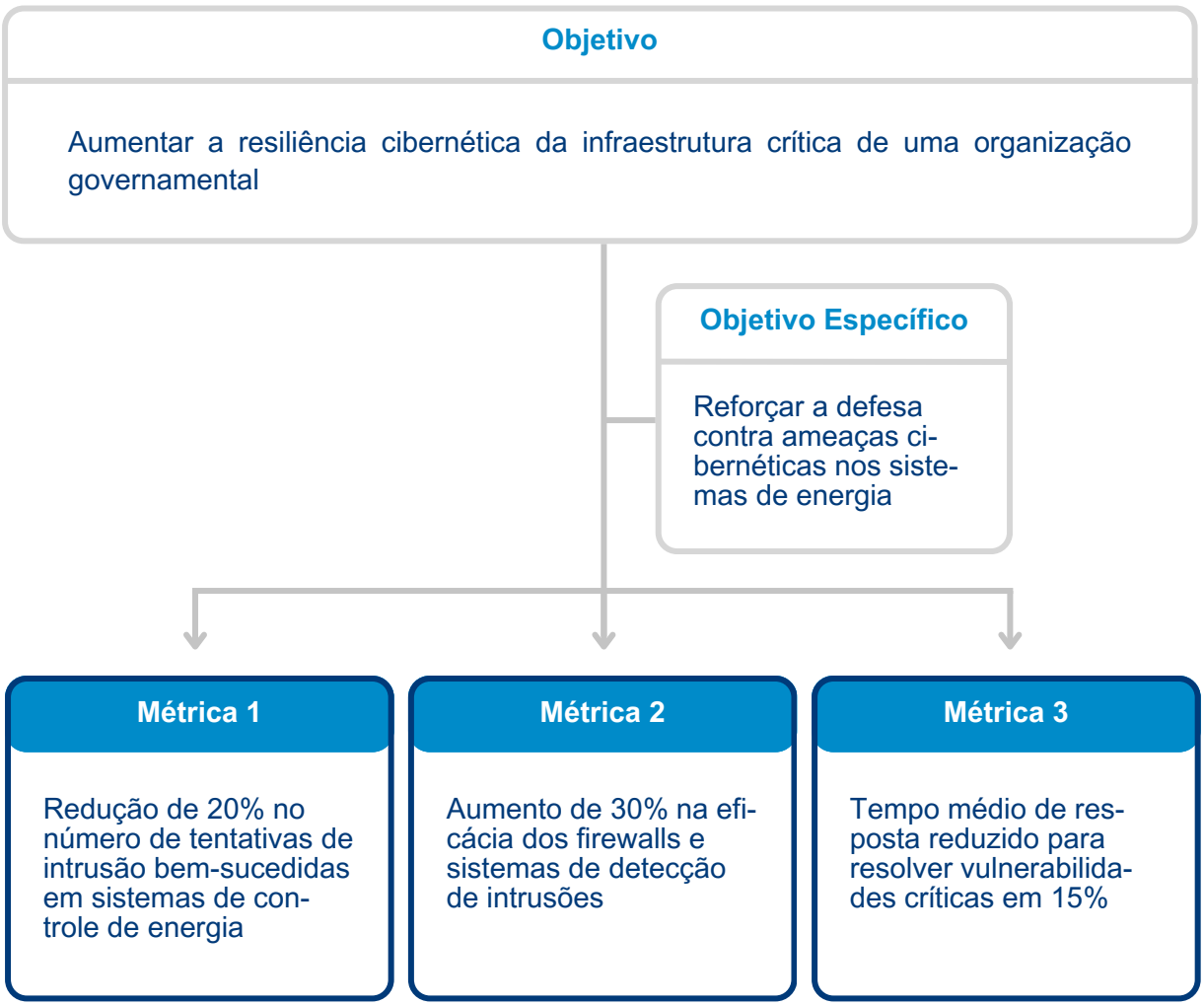
- 'Validar' *[ação]* os 'protocolos de cooperação estabelecidos previamente entre distintas áreas governamentais' *[processo a ser acionado]* frente à um 'incidente cibernético que tenha impactado o correto funcionamento das infraestruturas críticas de comunicação em nível nacional' *[contexto hipotético]*;
- 'Explorar' *[ação]* a execução de 'respostas de procedimento' *[processo a ser acionado]* frente a 'ocorrência de incidentes cibernéticos capazes de impactar infraestruturas críticas de comunicação em um determinado estado geográfico' *[contexto hipotético]*;
- 'Reforçar' *[ação]* 'mecanismos de compartilhamento de informações' *[processo a ser acionado]* entre 'organizações privadas e órgãos de segurança pública' *[contexto hipotético]*; e
- 'Exercitar' *[ação]* a 'procedimentos de recuperação de dados críticos' *[processo a ser acionado]* após 'ataques cibernéticos direcionados a informações sensíveis de uma base de dados específica' *[contexto hipotético]*.

Cada objetivo específico deve ser acompanhado por métricas e indicadores que facilitem a avaliação do desempenho.

Exemplo

Considere o objetivo de "testar o nível de cooperação entre dois ou mais departamentos de uma organização em uma simulação de ameaça cibernética", que se desdobra no objetivo específico de "monitorar as ocorrências de cooperação em um contexto simulado de escalada de crise".

Métricas como o "número de chamados de cooperação", "número de reuniões e teleconferências realizadas" ou "número de ações desenhadas em conjunto" ajudam a quantificar e mensurar o sucesso do objetivo específico.


Objetivo
Aumentar a resiliência cibernética da infraestrutura crítica de uma organização governamental
Objetivo Específico
Reforçar a defesa contra ameaças cibernéticas nos sistemas de energia
Métrica 1
Redução de 20% no número de tentativas de intrusão bem-sucedidas em sistemas de controle de energia
Métrica 2
Aumento de 30% na eficácia dos firewalls e sistemas de detecção de intrusões
Métrica 3
Tempo médio de resposta reduzido para resolver vulnerabilidades críticas em 15%

5) Definição do escopo

Para efeito desse item, o termo escopo do exercício refere-se às atividades de simulação que serão desenvolvidas no contexto do exercício de cibersegurança. Trata-se de um subconjunto das atividades necessárias para a realização do exercício como um todo, que compreendem, também, planejamento, logística etc.

O escopo do exercício é uma parte crucial da fase de planejamento, delineando os limites e o conteúdo do exercício (simulação).

Em primeiro lugar, requer a definição das dimensões que comporão o exercício, caracterizadas na Seção 2.

Em segundo lugar, requer a definição das áreas da organização que serão envolvidas.

Finalmente, envolve a previsão dos processos relevantes a serem utilizados ou desenhados durante as atividades do exercício – como planos de resposta a incidentes cibernéticos; políticas, regulamentos e legislações pertinentes; protocolos de gestão de crise e cooperação interdepartamental etc. – bem como a explicitação dos processos que ficarão de fora do escopo, identificando aquilo que será ou não alcançado pelo exercício.

Esta abordagem é essencial para o processo de articulação prévio, prevenindo distrações e mantendo o foco em atividades críticas. Em outras palavras, a adequada definição do escopo possibilita que o exercício seja elaborado e desenvolvido com a dimensão e propósito adequados, norteando a orientação da equipe de planejamento.

6) Definição dos participantes

A definição dos participantes é um desdobramento da definição do escopo do exercício (simulação). A partir deste escopo, é necessário determinar o perfil dos participantes, tanto em relação à sua capacidade técnica (mais ou menos especializado na temática da cibersegurança) quanto em relação aos cargos que desempenham no âmbito da organização (mais operacional ou gerencial, ou misto). O número de participantes desponta como uma questão relevante, com sua delimitação ficando condicionada ao tamanho e complexidade almejados para o exercício.

7) Definição do cronograma

A definição do cronograma é um desdobramento da definição do escopo e dos participantes do exercício. Deve dimensionar as necessidades de tempo consideradas indispensáveis à realização de todas as atividades previstas para a realização do exercício como um todo.

No que refere especificamente à realização do exercício (simulações), de forma geral durações muito extensas tendem a torná-los improdutivos. De forma geral, os exercícios de segurança cibernética têm duração de 2 dias podendo variar de 4 a 8h por tempo de atividade.

Cabe observar que a métrica para a definição da duração do exercício não precisa ser, necessariamente, temporal. Por exemplo, o exercício pode se encerrar, antes do prazo definido, caso seu objetivo seja atingido.

Logicamente, ajustes finos nesse cronograma deverão ser realizados mediante a conclusão dos planejamentos específicos das atividades de preparação logística (Seção 3.3) e preparação técnica (Seção 3.4).

Apenas a título de exemplo, a Figura 4.1.2 apresenta o cronograma referente a um exercício de cibersegurança planejado para ocorrer em um prazo de seis meses e considerando mais dois meses para a atividade de avaliação geral e desenvolvimento.

Atividades

A. Formação da equipe de planejamento
B. Identificação do propósito do exercício
C. Estabelecimento de metas e objetivos
D. Determinação dos objetivos específicos
E. Definição do escopo
F. Definição dos Participantes
G. Definição do cronograma
H. Elaboração de documentação referencial
I. Formação da equipe de coordenação geral
J. Coordenação da logística e da operação
K. Coordenação das interfaces com *stakeholders*
L. Acompanhamento da execução e ajuste fino do escopo e cronograma
M. Avaliação final e Plano Melhorias
N. Formação da equipe de logística
O. Planejamento e preparação
P. Formação da equipe técnica
Q. Estruturação da dinâmica de simulação
R. Treinamento da equipe de execução
S. Preparação dos participantes
T. Apoio logístico
U. Execução técnica

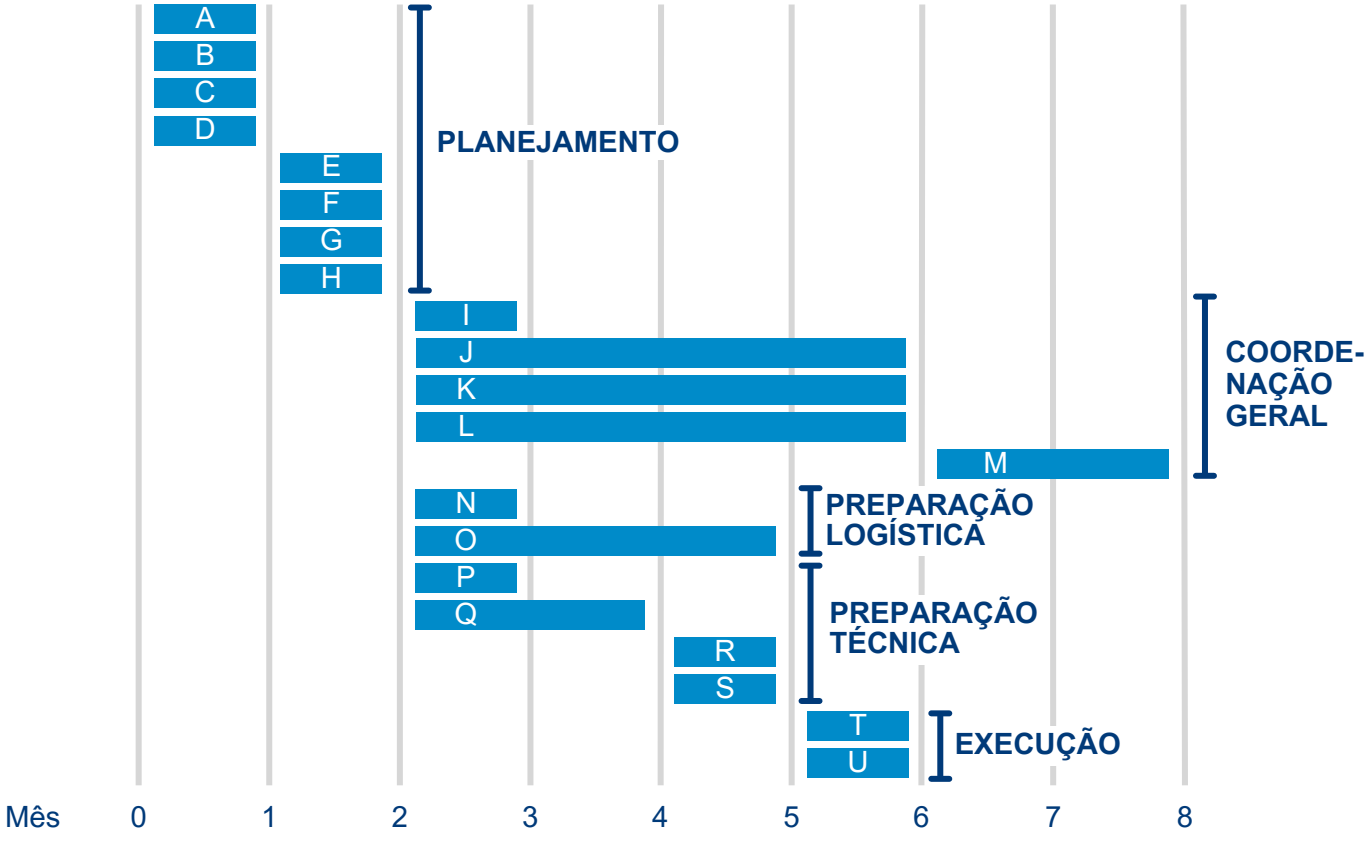


Figura 4.1.2
Exemplo de cronograma

8) Elaboração de documentação referencial

Refere-se à preparação da documentação referencial necessária à execução do exercício. Este processo também desempenhará papel fundamental para a posterior replicação do evento, estruturando as bases para o seu aperfeiçoamento e progresso no decorrer de suas futuras edições.

Os principais documentos referenciais são:

- **Diário de planejamento:** Fornece as principais atividades-chave inerentes ao planejamento e sua execução, incluindo registros das reuniões para a identificação dos propósitos, a definição do escopo, o estabelecimento de metas e objetivos, o formato do exercício, as áreas mobilizadas, a logística empreendida, a definição do público-alvo e todo e qualquer processo que se vincule à organização e realização do evento;
- **Carta de intenção:** Serve como guia oficial, descrevendo o propósito do exercício e suas metas, objetivos e métricas, bem como as necessidades organizacionais que se pretende atender;
- **Convite oficial:** Modelo de convite a ser enviado aos participantes. Devem conter instruções claras sobre datas, horários, localização, requisitos de segurança e quaisquer outras informações práticas pertinentes;
- **Manual do exercício:** Deve ser entregue preferencialmente junto com o convite, introduzindo de antemão aos participantes à dinâmica prevista no evento. Nesse sentido, deve apresentar informações acerca do cenário hipotético, pano de fundo, estrutura das atividades que serão realizadas e todo e qualquer material utilizado para contextualizar o exercício. É fundamental que as informações disponibilizadas contribuam para motivar os participantes, enfatizando as capacidades a serem desenvolvidas, mas sem adentrar nos detalhes acerca da descrição mais específica dos incidentes cibernéticos que serão trabalhados – resguardando, assim, os elementos de imprevisibilidade, surpresa e complexidade que deles se esperam;
- **Programação pré-definida:** Deve ser igualmente entregue junto com o convite, especificando todas as atividades pré-definidas do exercício. Importante incluir um evento de boas-vindas e uma reunião de orientação geral prévia que reforce o detalhamento das atividades a serem realizadas e permita uma primeira interação direta com os participantes confirmados, dirimindo dúvidas adicionais e reforçando as regras e procedimentos básicos que devem ser seguidos – incluindo diretrizes e limites da atuação, o respeito às políticas internas e a conformidade com as regulamentações vigentes; e
- **Guia de comunicação:** Documento restrito à equipe de planejamento, especificando as estratégias de comunicação interna e, dependendo da organização, junto a outros *stakeholders*, tais como o governo, órgãos reguladores, ONGs e imprensa.

Tendo em vista a importância dos seus registros, a documentação referencial deve ser mantida atualizada e acessível.

4.2 Coordenação Geral

Por não ser constituir em uma atividade a ser desenvolvida continuamente pela organização, os exercícios de cibersegurança envolvem uma atividade de gestão da execução, aqui denominada de coordenação.

É comum que as atividades de coordenação sejam consideradas como parte da atividade de planejamento e, de fato, conforme mencionado na Seção 4.1, quando concluído o planejamento propriamente dito, a equipe do planejamento integrará as equipes de coordenação geral, de coordenação logística e de coordenação operacional.

No contexto aplicado aos exercícios de cibersegurança, a coordenação geral envolve as seguintes atividades:

1) Formação da equipe de coordenação geral;

2) Coordenação da logística e técnica;

3) Coordenação das interfaces com *stakeholders*;

4) Acompanhamento da execução e ajuste fino do escopo e cronograma; e

5) Avaliação final e Plano de Melhoria.

1) Formação da equipe de coordenação geral

A principal função da coordenação geral é gerir a execução do planejamento estabelecido.

De forma geral, a equipe de coordenação geral deve abranger, no mínimo, as seguintes funções:

- Coordenador geral: Tem a responsabilidade de gerir o exercício e se reportar às esferas superiores da organização; e
- Assessor de planejamento: Tem a responsabilidade de acompanhar a execução do escopo, do cronograma e do orçamento estabelecidos na etapa de planejamento.

É recomendável que se avalie cuidadosamente quem deve fazer parte do time e que seja uma quantidade gerenciável de pessoas. Baseado no objetivo do exercício, devem ser identificadas as áreas da organização que possam ceder colaboradores.

2) Coordenação de logística e técnica

Na medida em que a “linha de frente” da gestão das atividades caberá às coordenações com atribuições logísticas e técnicas, caberá ao coordenador geral orientar, mediar e controlar as ações desses atores.

A critério da organização, o Coordenador Geral pode acumular a função dos coordenadores logístico e/ou técnico.

3) Interfaces com stakeholders

Dependendo das caraterísticas da organização, poderá ser maior ou menor a necessidade de comunicação e interação com *stakeholders* externos em relação ao exercício de segurança cibernética (governo, órgãos reguladores, ONGs etc. e, dependendo da organização, a imprensa).

Em grande medida, se a necessidade for maior, é possível que a organização já disponha de estruturas capazes de geri-las. De toda forma, caberá a coordenação geral responsabilizar-se ou articular-se com as áreas responsáveis para que as interfaces com *stakeholders* externos sejam realizadas.

4) Acompanhamento da execução e ajuste fino do escopo e cronograma

A Coordenação Geral deverá acompanhar a todas as atividades relacionadas ao exercício, reportando-se às instâncias superiores da organização. Trata-se de acompanhar a execução e zelar pelo cumprimento do escopo, do cronograma e do orçamento estabelecidos na etapa de planejamento.

É natural que, ao longo do processo de acompanhamento do planejamento, eventuais adaptações e readaptações sejam realizadas, refletindo as necessidades, disponibilidades e limites encontrados. Neste sentido, a flexibilidade desponta como um fator crucial para a execução da coordenação.

5) Avaliação final e Plano Melhoria

Tomando por base o Relatório Pós-Ação (vide seção 4.5, item 2, subitem Reunião Pós-Ação), uma análise de dados deverá ser conduzida para determinar se os participantes atingiram os objetivos propostas. Essa avaliação deverá documentar os pontos fortes e fracos, identificando áreas para melhoria do exercício

Independentemente do formato de simulação adotado, devem ser comparados os objetivos do exercício com o desempenho efetivo dos participantes, identificando as capacidades que precisarão de aprimoramentos.

Para isso, questões como o alinhamento com os planos, políticas e procedimentos atuais, impacto das diferenças e avaliação das consequências de ações (ou inações) são essenciais. Os pontos fortes e as áreas de melhoria devem ser identificados para remediar deficiências.

A partir do Relatório Pós-Ação, é desenvolvido um Plano de Melhorias, moldando as prioridades e a preparação da organização para futuros exercícios. Esse relatório inclui:

- Ações necessárias para abordar áreas de melhoria e recomendações associadas
- Colaboradores responsáveis por implementar medidas corretivas; e
- Cronogramas para conclusão de cada ação corretiva.

Dica

A continuidade da realização dos exercícios de cibersegurança no longo prazo desponta como um elemento fundamental para o desenvolvimento da maturidade cibernética no âmbito das organizações, criando oportunidades para que as áreas participantes e corpo técnico aprimorem cada vez mais suas capacidades de resiliência, adaptação e prontidão frente à um horizonte de ameaças constantes, crescentes e ininterruptas.

Desde a primeira edição do exercício, é fundamental que se estruture as bases para a sua posterior replicação. Este processo deve ser incremental, com cada edição sendo construída com base na anterior.

Isso envolve integrar os ciclos de planejamento, execução, avaliação e aperfeiçoamento em um plano de gerenciamento plurianual que contemple a evolução contínua do exercício.

A ideia se ter em mente é que, com um programa de gerenciamento plurianual efetivo, cada edição do exercício se torne um componente da engrenagem que viabilizará a concretização de um programa de resultados maior, com suas respectivas prioridades e aspirações.

4.3 Preparação logística

No contexto das atividades inerentes aos exercícios de cibersegurança, a atividade logística refere-se ao suprimento da infraestrutura e dos serviços, em grande medida de natureza temporária, necessários à sua realização.

Nesse contexto, a complexidade de seu escopo e a amplitude estarão fortemente condicionados ao escopo tamanho e à dimensão propostos para o exercício e às particularidades da organização. Por exemplo:

- Se, por um lado, o exercício pode ter como público-alvo uma área ou várias áreas da organização, uma área pode ter potenciais participantes espalhados geograficamente ou várias áreas podem estar localizadas em uma mesma cidade; e

- A organização pode dispor ou não de equipamentos e infraestruturas de apoio (auditório, salas, refeitório etc.) para a realização do exercício.

Em qualquer caso, uma vez que a duração dos exercícios de cibersegurança, que requerem a interrupção das atividades regulares dos participantes, precisa ser curta (via de regra, limitada a alguns dias), é crucial que problemas de natureza logística não prejudiquem o desenvolvimento das atividades segundo o escopo e cronograma estabelecidos.

No contexto mais específico aplicado aos exercícios de cibersegurança, a preparação logística envolve as atividades de: Formação da equipe de logística; e Planejamento e preparação.

1) Formação da equipe de logística

A equipe de logística deve ser formada, inicialmente, pelos responsáveis pelo planejamento da logística, aos quais caberá detalhar as ações previstas na etapa de planejamento.

Concluído o planejamento, que deverá definir as atividades que serão realizadas diretamente pela organização, delimitando as estruturas pré-existentes para assumi-las e as atividades que serão contratadas, estarão disponíveis elementos para dimensionar a equipe de logística.

De toda forma, a equipe logística deve abranger, no mínimo, as seguintes funções:

- **Coordenador logístico:** Tem a responsabilidade de planejar e gerir a logística do exercício e se reportar à coordenação geral; e
- **Facilitadores logísticos:** Tem a responsabilidade de orientar os participantes, sanar eventuais dúvidas, identificar e reportar não conformidades e problemas e contribuir com ações estabelecidas para solucioná-los. Devem ter experiências compatíveis com as áreas em que vão atuar (por exemplo, infraestrutura de TI, transporte e acomodações dos participantes ou alimentação).

A critério da organização, o Coordenador geral pode acumular a função do Coordenador logístico.

É recomendável que se avalie cuidadosamente quem deve fazer parte do time e que seja uma quantidade gerenciável de pessoas. Baseado no objetivo do exercício, devem ser identificadas as áreas da organização que possam ceder colaboradores.

2) Planejamento e preparação

Garantir a estrutura logística é vital para manter o escopo, ritmo e a integridade na execução do exercício. Esta estrutura depende de elementos essenciais, como o treinamento dos facilitadores logísticos, a estruturação de sistemas de suporte, comunicação e monitoramento e uma sólida cadeia de comando.

Dentre as etapas indispensáveis para a condução da logística, destacam-se:

- **Detalhamento do planejamento:** Deve planejar em detalhes todos os aspectos indispensáveis às atividades logísticas que serão realizadas, a distribuição de materiais, as equipes de suporte que ficarão de plantão durante a execução do exercício e a organização de ensaios e treinamentos necessários para todos os envolvidos. Esta preparação abrange a distribuição de documentação aos participantes, instruções adicionais e a criação de processos de contingência. Abrange, também, a definição dos responsáveis pela realização da atividade, que podem ser membros da equipe de logística, de outras áreas da organização ou prestadores de serviços contratados;

- **Configuração de instalações:** Recomenda-se ajustar a configuração das instalações com base na disponibilidade de recursos e sistemas de infraestrutura e na escolha do formato do exercício, proporcionando ambientes adequados para conferências, seminários, oficinas e simulações. Isso inclui a utilização de equipamentos apropriados de audiovisual para facilitar a comunicação e a visualização, como televisões, projetores, telas de projeção, microfones e caixas de som. Importante destacar também que o formato das salas impacta diretamente na comunicação entre os participantes, desempenhando papel fundamental na execução eficiente do exercício. Este formato, seja físico ou virtual, estabelece parâmetros para cenários realistas e contribui para a credibilidade do exercício, orientando seus planejadores em direção à concretização das metas e objetivos assumidos. Por fim, é imperativo assegurar que todas as máquinas estejam equipadas com os sistemas operacionais, softwares e componentes necessários ao exercício, incluindo servidores, roteadores, firewalls, máquinas virtuais etc.;

- **Contratação externa ou interna de espaços, equipamentos e serviços:** A contratação externa refere-se à atividade de *procurement* para fazer frente às necessidades do exercício que não possam supridas pela própria organização. A contratação interna refere-se à articulação e definição de responsabilidades com as áreas da própria organização que possam suprir as necessidades do exercício. Vale notar que a própria atividade de *procurement* pode ser contratada internamente;

- **Preparação antecipada:** Antes da execução do exercício, devem estar finalizados todos os aspectos indispensáveis às atividades logísticas que serão realizadas, incluindo a distribuição de materiais e a organização de ensaios e treinamentos necessários para todos os envolvidos, com destaque para os facilitadores logísticos. Esta preparação abrange a distribuição de documentação aos participantes, instruções adicionais e a criação de processos de contingência que devem estabelecer protocolos para situações excepcionais; e

- **Teste da estrutura montada:** Todos os recursos empregados na execução do exercício devem ser meticulosamente testados de modo a prevenir falhas e intercorrências que comprometam a adequada condução do exercício. Em particular, é imperativo:

  1) Certificar fontes de energia adicionais, como geradores e baterias, para assegurar a continuidade do exercício frente à possibilidade de falhas técnicas;

  2) Realizar backups de sistemas críticos é uma prática essencial para evitar contratempos inesperados, recuperando dados de forma eficiente e minimizando o impacto de eventuais perdas nos processos da organização; e

  3) Testar infraestrutura de sistemas e rede de forma a garantir a estabilidade da conectividade, principalmente no caso da simulação virtual.

Dica

Nos casos em que o exercício ocorra simultaneamente em diferentes localidades geográficas, é essencial assegurar um cuidado adicional no que se refere a adequada coordenação e sincronização do fluxo de informações.

4.4 Preparação técnica

A preparação técnica corresponde a concepção do exercício propriamente dito. Conforme apresentado na Seção 3, os exercícios de cibersegurança podem envolver um dos seguintes formatos, ou ambos: simulação construtiva e simulação virtual.

No contexto aplicado aos exercícios de cibersegurança, a preparação técnica envolve as atividades de: Formação da equipe técnica; Estruturação da dinâmica de simulação; Treinamento da equipe de execução; e Preparação dos participantes.

1) Formação da equipe técnica

Uma vez definidos, na fase de planejamento, a estrutura e o desenho geral da simulação, sua posterior e bem-sucedida execução dependerá de alguns atores-chave. Neste processo, é fundamental que os colaboradores sejam exaustivamente treinados para o desempenhar suas funções.

De forma geral, a equipe técnica deve abranger, no mínimo, as seguintes funções:

- **Coordenador técnico:** Tem a responsabilidade de estruturar a dinâmica da simulação, conduzir sua implementação e se reportar à coordenação geral;
- **Facilitadores técnicos:** Trabalham sob a supervisão e direcionamento do coordenador técnico, contribuindo para a execução das atividades atinentes ao exercício de simulação às quais estão diretamente envolvidos;
- **Mediadores:** Responsáveis pela execução da linha cronológica de ações e eventos da simulação (*Master Scenário Event List* - MSEL). Nesse sentido, devem introduzir os contextos relativos às simulações e conduzir as atividades práticas e discussões cabíveis, garantindo seu formato sequencial, cronológico, imersivo, realista e desafiador, no sentido de direcionar os participantes para a elaboração de soluções detalhadas. Neste aspecto, é imprescindível que detenham uma compreensão minuciosa de todos os elementos estabelecidos durante a etapa de estruturação da dinâmica da simulação;
- **Coletores de dados:** A coleta de dados da condução da dinâmica da simulação é vital. Estes colaboradores devem dominar profundamente os parâmetros de avaliação estabelecidos na linha cronológica de ações e eventos da simulação (MSEL), em suas métricas e indicadores, para que possam observar, coletar e registrar as impressões e resultados alcançados pelos participantes durante a realização da simulação;
- **Avaliadores:** A partir da coleta de dados e dos parâmetros de avaliação estabelecidos, os avaliadores se responsabilizarão pela avaliação das decisões e soluções propostas pelos participantes durante a simulação, comparando os objetivos do exercício com o desempenho real observado. Também desempenham papel importante na identificação das capacidades que precisam ser aprimoradas. Para isso, questões como o alinhamento com os planos, políticas e procedimentos atuais da organização, impacto das diferenças e avaliação das consequências de ações (ou inações) são essenciais. Tal como os demais colaboradores, devem compreender e dominar todos os elementos da linha cronológica de ações e eventos da simulação (MSEL), em suas métricas e indicadores.

A despeito da separação de papéis aqui sugerida, é perfeitamente possível que haja uma acumulação de funções entre estes colaboradores, se entendida como relevante pela organização em face aos limites de recursos ou preferências.

A critério da organização, o Coordenador geral pode acumular a função do Coordenador técnico.

É recomendável que se avalie cuidadosamente quem deve fazer parte do time e que seja uma quantidade gerenciável de pessoas. Baseado no objetivo do exercício, devem ser identificadas as áreas da organização que possam ceder colaboradores.

2) Estruturação da dinâmica de simulação

Conforme já abordado ao longo deste Manual, uma atividade fundamental para o sucesso do exercício é a estruturação do formato, do conteúdo e das atividades das simulações – em suma, todos os elementos de sua dinâmica.

Dessa forma, é imprescindível que o coordenador técnico e os facilitadores responsáveis por esta área sejam especialistas e detenham avançados conhecimentos técnicos relacionados ao setor da cibersegurança, bem como um profundo entendimento acerca da dinâmica, dos propósitos e objetivos estabelecidos para o exercício. Devem ter credenciais que os habilitem e gerem respeito junto aos participantes

Durante a simulação, o coordenador técnico assume a função de um “Senhor da Guerra” ou “Maestro”. Ele é o dono da sala de guerra e sua missão é dar o ritmo das ações.

Já os facilitadores devem ter habilidade para não gerar fricções desnecessárias e, ainda, não inibir a contribuição dos participantes.

É importante que se crie a linha cronológica de ações e eventos da simulação (MSEL), com vista a guiar a equipe responsável pela sua execução e, paralelamente, estimular a atuação dos participantes. Tal linha cronológica de ações e eventos da simulação (MSEL), é fundamental para garantir que os eventos aconteçam ordenadamente e viabilizem a concretização dos objetivos para os quais foram desenhados.

Uma adequada linha cronológica de ações e eventos da simulação (MSEL), deve contemplar os seguintes elementos:

- **Cenário realista:** As simulações devem refletir cenários que desafiem a capacidade de gestão de crise dos participantes, incorporando elementos de imprevisibilidade, surpresa e complexidade. O desafio está em atender a todos esses requisitos, concebendo uma simulação rica e envolvente. Trata-se de um processo meticuloso, projetado para ser introduzido em estágios, com níveis crescentes e escalonados de complexidade, abarcando todo um sequenciamento intermediário de eventos interconectados até a fase de retorno à normalidade;

- **Problemas cibernéticos simulados (PCS):** Situação fictícia criada para simular um incidente de segurança cibernética com o objetivo de treinar e propiciar a avaliação das respostas e habilidades dos profissionais na área de cibersegurança. Esses PCS podem ser baseados em ataques reais anteriores, tendências observadas ou objetivos específicos de treinamento, a depender da proposta e formato da simulação. Também é crucial que estejam alinhados aos objetivos e necessidades da organização e sejam realistas e relevantes para o seu ambiente operacional; e

- **Parâmetros de avaliação:** Deverão estar alinhados aos objetivos estabelecidos para o exercício e alicerçados em métricas e indicadores que proporcionem uma estrutura de avaliação precisa de desempenho dos participantes em termos de capacidades cibernéticas e resultados alcançados.

Embora seja compreensível que aspectos mais gerais do cenário possam ser apresentados antecipadamente aos participantes, de forma a contextualizar o exercício, o mesmo não pode ser dito da linha cronológica de ações e eventos da simulação (MSEL), que deve permanecer restrita apenas à equipe que conduzirá o planejamento e a execução do exercício. Tal precaução se deve à necessidade de se resguardar ao máximo os elementos de imprevisibilidade, surpresa e complexidade que se esperam dos incidentes cibernéticos simulados e dos eventos desencadeados por eles.

Exemplo

Cenário: Uma simulação de ataque cibernético em uma instituição financeira, onde os participantes enfrentam uma série de desafios, como tentativas de *phishing*, exploração de vulnerabilidades e ataques de *ransomware*.

O cenário ainda pode incluir eventos imprevisíveis, como interrupções de energia e a indisponibilidade de sistemas críticos, visando testar a resiliência e a capacidade de resposta nestas condições. Isso acrescenta complexidade ao cenário, exigindo adaptação imediata por parte dos participantes. Neste caso, é importante que tais eventos sejam cuidadosamente incorporados à linha cronológica de ações e eventos da simulação (MSEL) de modo a garantir a integração e a fluidez da simulação.

Problemas cibernéticos simulados (PCS): Com base no cenário proposto, uma linha cronológica de ações e eventos da simulação (MSEL) poderia descrever a seguinte sequência de eventos interconectados:

- Inicialmente, os participantes recebem alertas de atividades suspeitas;
- Em seguida, enfrentam uma onda de ataques de *phishing* que resultam no comprometimento de credenciais;
- Conforme a simulação avança, há um vazamento de dados e um pedido de resgate por meio de *ransomware*;
- Na medida em que os participantes atuam na resolução dos problemas, deve-se observar se as condições que indicam o término da simulação e o retorno à normalidade foram satisfatoriamente atendidas.

Parâmetros de Avaliação: Para a simulação mencionada, os parâmetros de avaliação incluiriam a eficácia na detecção e resposta a incidentes, o tempo de recuperação de sistemas essenciais, a precisão na identificação de ameaças, e a conformidade com políticas de segurança. Métricas específicas podem ser estabelecidas, como tempo médio de resposta, taxa de detecção de *phishing* e sucesso na restauração de serviços críticos.

3) Treinamento da equipe de execução

A adequada execução de exercícios de simulação depende do fornecimento no timing adequado de inputs para os participantes. Além disso, a existência de participantes com nenhuma ou pouca experiência prévia em atividades dessa natureza requer que os responsáveis por orientá-los previnam a ocorrência de situações que possam prejudicar o ritmo do exercício.

Cabe notar que os exercícios envolvem um grau razoável de complexidade técnica, implicando que, mesmo que já detenham a expertise adequada, os facilitadores técnicos, mediadores, coletores de dados e avaliadores devem ser exaustivamente treinados para a implementação dos procedimentos sob suas responsabilidades.

Os escopos dos treinamentos não se constituem em problema, na medida em que se tenha domínio do processo do exercício. Contudo, a condução dos treinamentos, no caso de exercícios de maior porte, pode exigir a alocação de profissionais especializados. No caso de exercícios de menor porte, essa atividade pode ser atribuída a coordenação técnica.

4) Preparação dos participantes

Esta atividade é considerada fundamental para garantir a boa condução das atividades no âmbito da simulação, permitindo que os participantes estejam completamente alinhados antes do início do exercício. Deve abranger:

- A disponibilização do Manual do exercício, a ser entregue preferencialmente no momento da distribuição dos convites aos potenciais participantes do exercício, apresentando informações acerca do cenário hipotético, pano de fundo, estrutura das atividades que serão realizadas e todo e qualquer material utilizado para contextualizar o exercício; e

- Uma reunião de orientação geral prévia, inserida no documento referencial “Programação pré-definida do evento” (vide item 8 da Seção 4.1), apta a reforçar o detalhamento das atividades a serem realizadas e permitir a interação direta com os participantes confirmados, dirimindo potenciais dúvidas adicionais.

4.5 Execução

A execução corresponde ao exercício propriamente dito e as equipes de logística e técnica, definidas nos itens 4.3 e 4.4, são responsáveis por sua condução.

No contexto aplicado aos exercícios de cibersegurança, a execução envolve as atividades de: Apoio Logístico; e Execução técnica.

1) Apoio logístico

No transcorrer do exercício, o apoio logístico desempenha um papel vital, assegurando seu êxito. O espaço destinado ao exercício deve estar preparado para acomodar participantes e equipamentos necessários, com a equipe de apoio logístico para intervir em caso de falhas de materiais.

Considerando as necessidades individuais de cada organização, é relevante providenciar uma área dedicada a serviços de alimentação e descanso para garantir o bem-estar dos participantes. O planejamento de pausas estratégias é essencial para prevenir fadiga e preservar a produtividade.

A equipe de apoio logístico também desempenha um papel crucial na manutenção de canais eficazes de comunicação interna, facilitando a pronta identificação e resolução de qualquer problema imprevisto. O relato rápido dessas situações permite uma resposta ágil, mantendo o fluxo contínuo do exercício cibernético e contribuindo para o alcance dos objetivos estabelecidos.

2) Execução técnica

A execução do exercício deve envolver as seguintes atividades:

A) Abertura do evento

Tem o propósito de criar uma atmosfera propícia para o início do exercício. Esse momento pode ser inaugurado formalmente com uma saudação de boas-vindas, expressando agradecimento pela participação dos envolvidos. Em seguida, são apresentados tanto a relevância quanto os objetivos que se almeja atingir ao longo do evento, enfatizando o conceito de fortalecimento da resiliência em cibersegurança dentro da organização.

Durante esta fase, proporciona-se uma visão geral dos cenários que serão simulados, elucidando os tipos de ameaças a serem enfrentadas. Destaca-se também a função específica de cada participante, enfatizando a contribuição única de cada um para o êxito do exercício.

É essencial esclarecer as regras e procedimentos básicos que devem ser seguidos, incluindo diretrizes e limites da atuação, reforçando o respeito às políticas internas e conformidade com as regulamentações vigentes.

A abertura do evento é também o momento oportuno para informar sobre os canais de comunicação disponíveis durante o exercício. Ressalta-se a importância da comunicação eficaz para uma resposta integrada e coordenada diante dos desafios cibernéticos propostos.

Como parte desse processo, é recomendável reservar um momento específico para perguntas e esclarecimentos de dúvidas, permitindo que os participantes estejam completamente alinhados antes do início oficial do exercício. Com essas etapas concluídas de maneira abrangente, a abertura do evento é então formalmente concluída, proporcionando uma base sólida para o desenvolvimento das atividades programadas.

B) Simulação Construtiva (caso prevista)

A abordagem de simulação construtiva no exercício corresponde à simulação de um ambiente de trabalho cotidiano, proporcionando uma representação prática e realista.

Inicia-se esta etapa com uma visão geral apresentada pela equipe de planejamento do exercício, destacando os objetivos específicos da simulação construtiva. Após essa apresentação, instruções e explicações detalhadas são fornecidas, reiterando as orientações sobre os papeis e responsabilidades de cada participante.

Após a fase introdutória, o facilitador descreve o cenário criado, fornecendo informações de pano de fundo relevantes para o exercício.

Vale ressaltar que o facilitador assegura a integridade do cronograma, garantindo que a dinâmica do exercício transcorra de maneira coesa e eficiente.

Um exemplo de cenário para simulação construtiva pode ser a propagação de um *malware* na empresa fictícia “Y”. Ocorre um ataque de engenharia social, enviando e-mails de *phishing* para os funcionários da empresa. Um funcionário, ao clicar em um link malicioso no e-mail, realiza o download de um vírus trojan, disfarçado como uma atualização de software. O vírus é então executado na máquina do funcionário, se espalhando pela rede e explorando vulnerabilidades para estabelecer uma conexão com o servidor de comando e controle controlado pelo atacante.

As ferramentas de segurança, como o antivírus, identificam as atividades suspeitas na máquina infectada, gerando um alerta automático que notifica a detecção do vírus. Após a identificação, a máquina infectada é isolada para conter a propagação, bloqueando a comunicação com o servidor. Uma análise forense é conduzida para investigar e determinar a origem do malware, a extensão da infecção e possíveis vulnerabilidades exploradas. As máquinas afetadas são restauradas e patches (atualizações) de segurança são aplicados para corrigir as vulnerabilidades identificadas.

Após o exercício, uma análise pós-simulação é realizada para identificar melhorias e ajustes de segurança alinhados com os objetivos específicos da organização, contribuindo para o aprimoramento da resiliência cibernética.

C) Simulação Virtual (caso prevista)

Na abordagem de simulação virtual, o exercício se configura como um treinamento específico, adaptado aos objetivos individuais de cada organização.

A fase inicial da simulação virtual começa com uma visão geral apresentada pela coordenação técnica, elucidando o propósito da simulação virtual. Após esta introdução, instruções detalhadas são fornecidas, reforçando as orientações sobre os papeis e responsabilidades de cada participante.

Após a fase introdutória, o facilitador técnico realiza uma apresentação detalhada do cenário, elaborado pela equipe de planejamento, fornecendo informações relevantes para o exercício. Vale ressaltar que o facilitador técnico desempenha um papel crucial na preservação da integridade do cronograma. Neste ponto, os times *red team* e *blue team* recebem o cenário e iniciam o exercício.

Um exemplo de cenário para simulação virtual pode ser um ataque de *ransomware* na empresa fictícia "X". Considerando que a organização manipula dados sensíveis de clientes, incluindo informações financeiras e pessoais, o cenário visa simular um ataque de *ransomware* para avaliar a resposta da equipe de segurança.

A simulação se inicia quando um funcionário recebe um e-mail de *phishing* contendo um anexo malicioso disfarçado como um documento de fatura. Ao abrir o anexo, um *malware* de *ransomware* é ativado, espalhando-se silenciosamente pela rede da empresa, explorando vulnerabilidades nos sistemas e impactando máquinas e servidores críticos. Os atacantes, então, iniciam o processo de cifragem de dados nos servidores afetados, exibindo uma mensagem de resgate que exige pagamento em criptomoedas para a recuperação dos dados criptografados.

A partir desse cenário, os defensores (*blue team*) são acionados devido às atividades suspeitas. Identificando as máquinas afetadas, a equipe procura conter a propagação, bloqueando as comunicações com os servidores de comando e controle de *ransomware*. Durante a simulação, o time também considera opções de negociação com os atacantes de *ransomware*, avaliando os riscos e benefícios.

Embora a negociação não ocorra efetivamente, o cenário simula as decisões tomadas pela equipe.

Após a contenção, o *blue team* realiza a restauração dos dados e sistemas afetados, fazendo backups seguros para a recuperação das informações. Em seguida, uma análise forense é conduzida para determinar como o *ransomware* invadiu a rede, identificando as vulnerabilidades e melhorando a prevenção dos sistemas.

Ao término do exercício, uma análise pós-simulação é realizada para avaliar a resposta dos defensores, identificando oportunidades de melhorias no enfrentamento de ameaças cibernéticas similares.

D) Apresentação dos resultados (APA)

A etapa de apresentação dos resultados (APA) é essencial para compartilhar dados, análises e colher aprendizados após a condução do exercício.

Após a simulação, aproveitando que ainda estão focados no exercício, a coordenação técnica reúne os participantes, os coletores de dados e os avaliadores para a consolidação e discussão de feedbacks em relação ao exercício. Essa atividade, pode ser chamada de *hot debriefing*.

O objetivo principal é documentar o conhecimento adquirido, tanto das experiências negativas quanto positivas, assimilando as lições aprendidas.

Estas lições aprendidas devem capturar e considerar as diferentes abordagens de segurança entre os participantes do exercício, expondo técnicas bem-sucedidas e deficiências no programa de TI da organização, proporcionando oportunidades de construção e aprimoramento.

E) Reunião Pós-ação

A Reunião Pós-ação, da qual devem participar representantes das equipes de coordenações geral, técnica e logística, tem como propósito gerar um Relatório Pós-ação, o qual deve incluir:

- Resumo das atividades durante o exercício;
- Análise de desempenho de atividades essenciais;
- Avaliação dos principais pontos fortes e áreas para melhoria; e
- Recomendações de aprimoramento baseadas em análises.

As questões sugeridas abaixo podem contribuir para nortear as discussões e a própria elaboração do Relatório Pós-Ação:

- Que mudanças nos planos e procedimentos podem melhorar o desempenho geral do exercício?
- Que mudanças nas estruturas organizacionais podem melhorar o desempenho geral do exercício?
- Que mudanças nos processos de gestão podem melhorar o desempenho geral do exercício?
- Que mudanças em equipamentos ou recursos podem melhorar o desempenho geral do exercício?
- O treinamento fornecido foi eficaz e melhorou o desempenho geral do exercício?

Esse relatório deve ser encaminhado posteriormente aos participantes e a Coordenação Geral. Caberá à Coordenação Geral, por deter uma perspectiva completa da realização do exercício, a elaboração do Plano de Melhorias, tendo o Relatório Pós-ação como insumo (vide Seção 4.2, item 5).

F) Encerramento

O encerramento ocorre após a conclusão, no âmbito da Coordenação Geral, do Plano de Melhorias (vide Seção 4.2, item 5). Pode abranger um evento ou apenas a emissão de uma declaração de encerramento do exercício mencionado os resultados Relatório Pós-Ação e do Plano de Melhorias.

Anexo 1

Higiene Cibernética

Em um contexto de crescentes ataques cibernéticos que põem em risco os pilares da cibersegurança (confidencialidade, integridade e disponibilidade), afetando tanto indivíduos quanto corporações e governos, uma das principais vulnerabilidades exploradas é o "analfabetismo digital" dos usuários, ou seja, a deficiência de uma higiene cibernética adequada.

Segundo dados do *Government Communications Headquarters* (GCHQ), serviço de inteligência britânico encarregado da segurança e da espionagem e contraespionagem nas comunicações, 80% dos ciberataques naquele país ocorrem em consequência de hábitos inadequados das vítimas – normalmente, funcionários das organizações.

Nesse sentido, a higiene cibernética pode ser associada à profilaxia – da mesma forma que lavar as mãos previne o surgimento de doenças infecciosas, as práticas de higiene cibernética podem ser eficientes na prevenção de ataques de engenharia social, *phishing, malwares*, vírus, *ransomwares*, perda ou corrupção de dados, dentre outras ameaças cibernéticas mais ou menos nocivas.

Por não apresentarem, de forma geral, um elevado grau de sofisticação, a importância das práticas de higiene cibernética é, muitas vezes, subdimensionada. Mas, em verdade, a adoção de boas práticas como um processo habitual e rotineiro são muito efetivas para a cibersegurança das organizações.

Dentre os elementos abarcados pela perspectiva da higiene cibernética, tem-se:

- Falta de conscientização, conhecimento e habilidades em cibersegurança;
- Falta de responsabilidade;
- Falta de políticas de conformidade;
- Incapacidade em seguir as melhores práticas em cibersegurança;
- Incapacidade em compartilhar responsabilidades;
- Colaboradores inconsequentes;
- Criminosos cibernéticos; e
- Vulnerabilidades de softwares.

No nível social e de governança, considerando-se uma perspectiva mais sistêmica da questão, pode-se ainda assinalar os seguintes elementos:

- Falta de profissionais em cibersegurança;
- Ineficiências na detecção e no devido tratamento penal de criminosos cibernéticos;
- Falta de um arcabouço legal apropriado para lidar com o problema;
- Falta de inovação em cibersegurança;
- Falta de comunicação e colaboração;
- Incapacidade de defesa e resposta aos incidentes cibernéticos;
- Falta de liderança;
- Falta de pesquisa direcionada ao tema;
- Ausência de conselhos/consultoria adequada; e
- Existência de vítimas, dentre as quais se incluem organizações, que não relatam incidentes cibernéticos (inclusive, para evitar danos reputacionais).

Entende-se, assim, que a adoção de práticas de higiene cibernética no dia-a-dia de uma organização não é mais uma opção: é impreterível para que se promova a conscientização necessária à proteção dos sistemas e dados contra ameaças virtuais crescentes em complexidade e, principalmente, capacidade de produzir danos.

Com base nas orientações do Center for Internet Security (CIS), organização americana sem fins lucrativos, dedicada a ajudar pessoas, empresas e governos a se protegerem contra ameaças cibernéticas generalizadas, apresentam-se a seguir recomendações destinadas prioritariamente a aumentar a cibersegurança em nível individual. Esse tipo de iniciativa é relevante pois, devido à transversalidade do ciberespaço, não há grandes distinções entre os indivíduos em seus níveis pessoais e profissionais, de forma que a mentalidade voltada para a higiene cibernética deve ser continuamente estimulada para a construção de um ecossistema digital mais seguro.

Sob a perspectiva do porte das organizações, é possível notar uma importante lacuna associada às questões orçamentárias.

Para grandes empresas, é comum que haja uma maior disponibilidade e prioridade de recursos para tratar temas relacionados à cibersegurança. No entanto, as empresas de menor porte enfrentam um cenário mais desafiador no que diz respeito ao montante destinado para investimentos nesta área. Não coincidentemente, estas empresas despontam como alvos preferenciais de ataques cibernéticos.

Para tornar esse cenário mais complexo, muitas empresas de menor porte integram a cadeia de suprimentos de empresas de maior porte e governos, podendo, assim, ser responsáveis pela ampliação de vulnerabilidades dos clientes e consumidores, tornando-se vetores de entrada de ataques.

Para lidar com tais restrições, muitas organizações governamentais e privadas oferecem iniciativas de baixo custo para mitigar os problemas de cibersegurança.

Algumas das mais reconhecidas internacionalmente são atreladas à família ISO 27000 e ao Instituto Nacional de Padrões e Tecnologias (NIST, em inglês) dos Estados Unidos, como o NISTIR-7621. Além disso, há recomendações que, apesar de não terem força de lei, têm se tornado uma exigência padrão de governos e grandes empresas, como o Cyber Essentials, um padrão de controles de cibersegurança que dialoga com os supracitados, baseado em 5 pilares, exigido para os fornecedores do governo britânico. Esses controles de segurança são:

- **Firewalls e gateways:** Impedem o acesso não autorizado de ou para redes privadas;
- **Configuração segura:** Garante que os sistemas sejam configurados da maneira mais segura possível, de acordo com as necessidades da organização;
- **Controle de acesso:** Assegura que apenas aqueles que devem ter acesso aos sistemas o façam no nível apropriado;
- **Proteção contra *malware*:** Garante que a proteção contra vírus e *malware* esteja instalada e atualizada, incluindo “listas negras” de sites; e
- **Gerenciamento de patches (atualizações):** Garante que a versão mais recente e suportada de aplicativos seja utilizada e que todos os patches necessários disponibilizados pelo fornecedor tenham sido aplicados.

Apesar da importância em se compreender os principais ataques e suas respectivas contramedidas possibilitadas pela higiene cibernética, vale observar que cada organização deve dispor de uma infraestrutura de segurança baseada em métricas contextualizadas à sua própria realidade. Tais métricas devem:

- Ser adaptadas à arquitetura de segurança e ao tamanho e necessidades organizacionais;
- Estar alinhadas aos requisitos regulatórios da região da organização;
- Ser complementadas por treinamentos que estejam dentro das possibilidades e do orçamento da organização;
- Ser manuteníveis e replicáveis com os recursos à disposição da organização; e
- Estar alinhadas, dando suporte aos objetivos operacionais e estratégicos do negócio

Assim, a higiene cibernética está diretamente ligada a práticas dos usuários e dos departamentos de tecnologia da informação com relação a manutenção de seus softwares e hardwares. Tais práticas devem ser devidamente observadas antes mesmo da implementação de soluções mais complexas, no sentido de garantir que o fator humano deixe de ser visto como um problema e passe a ser visto como uma solução em meio à esta complexa realidade.

Entendendo a higiene cibernética como um conjunto de boas práticas preventivas, tem-se à disposição um amplo acervo de medidas de baixo custo passíveis de serem adotadas para a mitigar os riscos inerentes às ameaças cibernéticas, com amplas possibilidades de implementação.

Demandam, para isso, uma campanha dedicada de conscientização, inclusive no nível estratégico das organizações, acerca da importância da infraestrutura de tecnologia da informação e da cibersegurança em nível individual não só para o bom andamento dos negócios por si só, mas para a promoção de um ecossistema cibernético mais seguro.

Apresentam-se a seguir exemplos de práticas de higiene cibernética para as organizações:

Pense antes de clicar

Passe o mouse sobre um link para revelar a URL de destino. Se parecer diferente do texto do hyperlink, é importante ter a consciência de não clicar nele. Pode ser uma tentativa de enganar o usuário, levando-o a visitar uma página de *phishing*. Para se proteger contra estes ataques, vale procurar pelo site desejado em um sistema de busca seguro ou inserir a URL diretamente na barra de navegação.

Não seja vítima de *phishing*

É importante que, ao receber um e-mail suspeito no trabalho, tenha-se a consciência de não abrir ou clicar em quaisquer itens que estejam anexados a ele. Um procedimento seguro nestas circunstâncias é entrar em contato imediatamente com o departamento de tecnologia da informação da organização.

Indo além da senha

Atores de ameaças cibernéticas (hackers maliciosos ou cibercriminosos) podem facilmente quebrar senhas como “senha”, “admin” ou “123456”. O mesmo vale para senhas baseadas em dicionário ou combinações de palavras que você pode encontrar em um dicionário. Nesse sentido, vale experimentar usar senhas que, às vezes, substitui números e símbolos por letras. Essa abordagem única pode ajudar a lembrar de sequências longas para uma segurança adicional.

Para garantir a segurança adequada de seus dispositivos e dados, é importante proteger os computadores e smartphones, entre outros dispositivos, com senhas seguras. Também é possível considerar o uso de biometria, sempre que possível, ou usar um PIN para autenticação.

Se é importante, use autenticação multifatorial (MFA)

Para implementar a autenticação multifatorial, é preciso proteger uma conta com mecanismos de autenticação de pelo menos duas das seguintes categorias:

- Algo que se sabe: uma senha ou padrão de deslize;
- Algo que se é: biometria, leitura de impressões digitais, facial etc.; e
- Algo que se tem: um aplicativo de autenticação no seu telefone ou um crachá de identificação.

É importante sempre utilizar, no mínimo, a autenticação de dois fatores (2FA) em contas importantes ou computadores onde dados sensíveis são manipulados. Dessa forma, mesmo que um cibercriminoso ganhe acesso às credenciais de acesso (nome de usuário e senha), não poderá acessar a conta sem o(s) outro(s) fator(es).

Mantenha-se atualizado

É fundamental sempre instalar as últimas atualizações do sistema operacional, navegador e quaisquer aplicativos instalados nos dispositivos. Hackers maliciosos podem explorar vulnerabilidades para acessar dispositivos conectados à uma mesma rede. Neste quesito, é imprescindível não se tornar um alvo fácil.

Reflita, depois conecte

Antes de se conectar a uma rede Wi-Fi desconhecida e/ou pública, é preciso considerar os riscos envolvidos, sobretudo no que tange ao compartilhamento indevido de dados. Para minimizar o risco desta exposição, use uma rede privada virtual (VPN, em inglês). Uma VPN age como um túnel seguro pela internet, criando uma conexão web criptografada e privada, em benefício de uma maior segurança para os dados pessoais.

Compras inteligentes, compras seguras

Fazer compras online é uma conveniência moderna e cotidiana. Proteger dados bancários sensíveis apenas comprando em sites confiáveis torna-se fundamental. É preciso ter a consciência de nunca salvar informações de pagamento onde possam ser roubadas e usadas posteriormente. Além disso, cabe se certificar se sempre monitorar os registros do cartão de pagamentos em busca de cobranças desconhecidas e/ou indevidas. Se encontrar algo suspeito, entre em contato com a administradora do cartão para contestar a cobrança e solicitar um novo cartão de pagamento.

Não seja um vetor de agressão

Estar online exige não apenas precauções, mas também responsabilidades. Compartilhar informações pessoais privadas de alguém online, prática conhecida como "*doxxing*," é inaceitável e pode resultar em problemas legais.

Carregue seus dispositivos móveis com cautela

Seja um dispositivo de trabalho ou pessoal, o carregamento de dispositivos móveis exige cautela. Carregá-los em estações públicas de carregamento USB pode tornar o portador do dispositivo uma vítima de "*juicejacking*", um tipo de ataque em que cibercriminosos infectam usuários desprevenidos com *malwares* ou roubo de dados. O uso de powerbanks ou o carregamento do dispositivo utilizando seu próprio cabo em uma tomada de parede tornam o procedimento mais seguro.

Esse foi apenas um panorama sobre o tema. Informações mais abrangentes e detalhadas, disponibilizadas pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), um dos serviços prestados para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço executivo do Comitê Gestor da Internet no Brasil (CGI.br), podem ser encontradas no endereço https://cartilha.cert.br/

Anexo 2

Para maior familiarização com os termos técnicos relacionados ao tema, alguns dos quais utilizados neste Manual, sugere-se consultar os seguintes glossários nacionais.

Glossário de Segurança da Informação
PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021
https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370

Glossário das Forças Armadas
PORTARIA NORMATIVA No 9/GAP/MD, DE 13 DE JANEIRO DE 2016
https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf

Anexo 3

Indicações bibliográficas

AUSTRALIA. A Guide to Cyber Exercises: Plan + Conduct + Evaluate. Victoria State Government. 2023. Disponível em: https://content.vic.gov.au/sites/default/files/2019-08/Vic-Gov-Cyber-Exercise-guide.pdf

BABIĆ, Vladan; BRATIĆ, Aleksandar. Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs. DCAF - Geneva Centre for Security Sector Governance. 2022. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents-/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf

CANADA. Exercise Design 100. Alberta Emergency Management Agency. 2012. Disponível em:https://open.alberta.ca/dataset/07935297-2c3d-4773-9028bbaf33fe98cf/resource/7361f1-a0-bc1c-4ee3-9f7c-e8cd7860b122/download/ma-exercise-design-100-course-manual.pdf

CERT.BR.Cartilha de Segurança para a Internet.Acesso em: 03 de setembro de 2024. Disponível em: https://cartilha.cert.br/

CIS. 11 Cyber Defense Tips to Stay Secure at Work and Home. Center for Internet Security. 2023. Disponível em: https://www.cisecurity.org/insights/blog/11-cyber-defense-tips-to-stay-secure-at-work-and-home

ELECTRIC POWER RESEARCH INSTITUTE. Guidelines for Leveraging NESCOR Failure Scenarios in Cyber Security Tabletop Exercises. 2014. Disponível em: https://smartgrid.epri.com/doc/Guidelines_For_Leveraging_Failure_Scenarios.pdf

ENISA. Cyber Europe 2022: After Action Report. European Union Agency for Cybersecurity. 2022. Disponível em: https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

ENISA. Review of Cyber Hygiene Practices. European Union Agency for Cybersecurity. 2017. Disponível em: https://www.enisa.europa.eu/publications/cyber-hygiene

GIBBY, Gordon. Exercise ViralDuo Master Scenario Events List (MSEL) Package. North Florida Amateur Radio Club. Disponível em: https://qsl.net/nf4rc/2019Conference/ExerciseViralDuoMSEL.pdf

KICK, Jason. Cyber Exercise Playbook. The MITRE Corporation. 2014. Disponível em: https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf

LIMOUSIN, Philippe et al. A New Method And Tools to Scenarios Design for Crisis Management Exercises. The Italian Association of Chemical Engineering. 2016. Disponível em: https://www.aidic.it/cet/16/53/054.pdf

MAENNEL, Kaie. et al. Cyber Hygiene: The Big Picture. In: Gruschka N. (ed) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science. Springer. 2018. DOI: https://doi.org/10.1007/978-3-030-03638-6_18

PETRIE, Michael. Homeland Security Exercise and Evaluation Program (HSEEP): Quick Reference Guide. University of California. Disponível em: https://www.calhospitalprepare.org/sites/main/files/file-attachments/cider_hseep_refgdv3.pdf?1376949630

RENGER, Ralph. et al. Steps in writing na effective Master Scenario Event List. Journal of Emergency Management. 2009. DOI: https://doi.org/10.5055/jem.2009.0039

SUCH, Jose M. et al. Basic Cyber Hygiene: Does It Work? Computer 52:4, p. 21-31. 2019. DOI: http://doi.org/10.1109/MC.2018.2888766

USA. CISA Tabletop Exercise Package Exercise Planner Handbook. Cybersecurity and Infrastructure Security Agency - Department of Homeland Security. 2020. Disponível em: https://www.cisa.gov/sites/default/files/publications/2%20-%20CTEP%20Exercise%20Planner%20Handbook%20%282020%29%20FINAL_508_1.pdf

USA. Homeland Security Exercise and Evaluation Program (HSEEP). Department of Homeland Security. 2020. Disponível em: https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

WEN, Shao-Fang; YAMIN, M. M.; KATT, Basel. Ontology-Based Scenario Modeling for Cyber Security Exercise. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2021. DOI: 10.1109/EuroSPW54576.2021.00032

WILHELMSON, Nina; SVENSSON, Thomas. Handbook for planning, running and evaluating information technology and cyber security exercises. National Defense College - Center for Asymmetric Threat Studies (CATS). 2013.

ZIMMERMANN, Verena; RENAUD, Karen. Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. In: International Journal of Human-Computer Studies, Vol. 131, pp. 169-187. 2019. DOI: https://doi.org/10.1016/j.ijhcs.2019.05.005

Anexo 4

Informações sobre o conteúdo das indicações bibliográficas

Exercícios de cibersegurança

Título	Informações sobre o conteúdo
A Guide to Cyber Exercises: Plan + Conduct + Evaluate	Visão resumida das etapas de um exercício de cibersegurança.
A New Method and Tools to Scenarios Design for Crisis Management Exercises	Artigo sobre métodos e ferramentas para desenvolvimento de cenários de exercícios de gerenciamento de crise.
CISA Tabletop Exercise Package Exercise Planner Handbook	Guia para exercícios Tabletop.
Cyber Europe 2022: After Action Report.	Modelo de Relatório Pós-Ação.
Cyber Exercise Playbook	Guia de fundamentos para exercícios de cibersegurança detalhando as etapas de planejamento e execução. Fornece *templates* e exemplos.
Exercise Design 100	Guia de desenvolvimento de exercícios para iniciantes. Inclui exercícios de autoavaliação.
Exercise ViralDuo Master Scenario Events List (MSEL) Package	Modelo de uma linha cronológica de ações e eventos da simulação (MSEL).
Guidelines for Leveraging NESCOR Failure Scenarios in Cyber Security Tabletop Exercises	Guia de fundamentos para exercícios de cibersegurança detalhando as etapas de planejamento e execução. Inclui uma seção de referências úteis.
Handbook for planning, running and evaluating information technology and cyber security exercises	Guia de fundamentos para exercícios de cibersegurança detalhando as etapas de planejamento e execução. Fornece exemplos e inclui seção com referências úteis.
Homeland Security Exercise and Evaluation Program (HSEEP)	Guia de fundamentos para exercícios de cibersegurança detalhando as etapas de planejamento e execução.
Homeland Security Exercise and Evaluation Program (HSEEP): Quick Reference Guide	Guia rápido de referências sobre o Homeland Security Exercise and Evaluation Program (HSEEP).
Ontology-Based Scenario Modeling for Cyber Security Exercise	Artigo sobre aspectos técnicos relevantes para a modelagem de cenários de simulação virtual.
Steps in writing an effective Master Scenario Event List	Artigo com instruções para a elaboração de uma linha cronológica de ações e eventos da simulação (MSEL).

Higiene Cibernética

Título	Informações sobre o conteúdo
Cartilha de Segurança para a Internet	Conjunto de materiais feita pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é um dos serviços prestados para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o braço executivo do Comitê Gestor da Internet no Brasil (CGI.br):https://cartilha.cert.br/
11 Cyber Defense Tips to Stay Secure at Work and Home	Práticas individuais de higiene cibernética.
Basic Cyber Hygiene: Does It Work?	Estatísticas sobre ataques a pequenas e médias empresas.
Cyber Hygiene: The Big Picture	Abordagens sobre higiene cibernética e dados quantitativos sobre o tema.
Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs	Medidas básicas de higiene cibernética para pequenas e médias empresas. Inclui uma seção com checklist.
Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset	Informações sobre o ambiente cibernético atual e proposição de um novo modelo considerando o humano como parte da solução.
Review of Cyber Hygiene Practices	Conjunto de medidas relacionadas à higiene cibernética comparando países da União Europeia.

Anexo 5

Atos Normativos

Decreto No 9.573, de 22 Nov 18 – Aprova a Política Nacional de Segurança de Infraestruturas Críticas (SIC);

Decreto No 9.637, de 26 Dez 18 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera (...);

Decreto No 9.819, de 03 Jun 18 – Dispõe sobre a CREDEN do Conselho de Governo;

Decreto No 10.222, de 05 Fev 20 – Aprova a Estratégia Nacional de Segurança Cibernética;

Decreto No 10.569, de 9 Dez 20 – Aprova a Estratégia Nacional de SIC;

Decreto No 10.748, de 16 Jul 21 – Institui a Rede Federal de Gestão de Incidentes Cibernéticos;

Decreto No 11.200, de 15 Set 22 – Aprova o Plano Nacional de SIC.

Portaria Normativa No 3.010/MD, de 18 Nov 14 – Aprova a Doutrina Militar de Defesa Cibernética;


COM-D CIBER


FGV