

Metodologia de defesa cibernética para organizações Versão 2.0

Práticas recomendadas em cibersegurança



A.02

Volume A:
Uma abordagem metodológica



Publicado originalmente pela Diretoria Cibernética Nacional de Israel em hebraico e inglês sob o título “Cyber Defense Doctrine. Managing the Risk: Full Applied Guide to Organizational Cyber Defense”.

© (2021) Estado de Israel - Diretoria Cibernética Nacional de Israel.

© (2022) Banco Interamericano de Desenvolvimento por esta tradução.

Este documento foi elaborado pela Diretoria Cibernética Nacional de Israel em hebraico e em inglês. A tradução ao português foi realizada pela equipe de cibersegurança da Divisão de Inovação nos Serviços ao Cidadão (IFD/ICS) do Banco Interamericano de Desenvolvimento (BID).

O leitor deve ter em mente que a cibersegurança é uma área em rápida evolução. Embora estes documentos reflitam princípios estabelecidos, eles podem ser atualizados periodicamente, conforme necessário, para refletir os desenvolvimentos na área. Além disso, embora tenham sido feitos todos os esforços para apresentar as recomendações e os recursos de maneira universalmente aplicável a organizações do mundo todo, o leitor poderá encontrar referências específicas ao ecossistema cibernético e ao contexto de Israel (como valores indicados em novos shekels israelenses [NIS] ou referências a regulamentações israelenses ou a seus órgãos governamentais).

Esta publicação pode ser baixada, copiada e distribuída, desde que seja dada a devida atribuição à Diretoria Cibernética Nacional de Israel para a versão original em hebraico ou inglês e ao BID para a tradução em português, e que a publicação não seja modificada. As opiniões expressas nesta publicação são de responsabilidade dos autores e não refletem necessariamente a posição do BID, de sua Diretoria Executiva ou dos países que representa.

O documento original está disponível no seguinte link: https://www.gov.il/en/Departments/General/cyber_security_methodology_2. Leve em conta que ali figura a seguinte declaração:

“Este documento foi elaborado pela Diretoria Cibernética Nacional de Israel com o objetivo de promover a defesa cibernética na economia israelense. Todos os direitos reservados à Diretoria Cibernética Nacional de Israel do Estado de Israel. Este documento foi elaborado como um serviço ao público. O ato de copiar o documento ou incorporá-lo a outros documentos está sujeito às seguintes condições: deve-se fazer referência à Diretoria Cibernética Nacional de Israel no formato listado abaixo; a versão mais recente do documento deve ser usada, sem nenhuma alteração no documento. O documento contém informações profissionais cuja implementação na organização exige um profissional de defesa cibernética informado sobre a organização e seus sistemas. Quaisquer comentários e referências ao documento podem ser enviados ao seguinte endereço de e-mail: tora@cyber.gov.il”.

Índice

Preâmbulo

/Pág. 2

Sumário executivo

/Pág. 8

01. Introdução

/Pág. 10

02. Princípios da metodologia de defesa cibernética

/Pág. 12

03. Estrutura da metodologia de defesa cibernética

/Pág. 14

04. Processo de planejamento através da lente da organização

/Pág. 20

Apêndices

/Pág. 69

Preâmbulo

A transformação digital e o desafio da cibersegurança

À medida que a transformação digital continua a se espalhar pelo mundo, governos, organizações, indivíduos e até mesmo objetos estão cada vez mais conectados à internet. Embora a digitalização tenha proporcionado benefícios inegáveis, como a prestação eficiente de serviços públicos, o crescimento econômico e a conectividade essencial para o desenvolvimento de inúmeras atividades, ela também contribui para a crescente exposição coletiva aos riscos de cibersegurança. Um dos principais impulsionadores desse fenômeno, nos últimos tempos, foi a pandemia global da COVID-19. Como resultado de políticas generalizadas de distanciamento social, o número de transações de comércio eletrônico e as comunicações pessoais on-line experimentou crescimento repentino e acentuado em curto período de tempo, em conjunto com o número de funcionários que começaram a trabalhar em regime de teletrabalho pela primeira vez. Nessa situação sem precedentes, muitos usuários da internet foram confrontados com novas interações on-line sem estarem sufi-

cientemente cientes dos riscos de segurança envolvidos. As organizações também tiveram que se adaptar rapidamente aos desafios, estabelecendo fluxos de trabalho totalmente remotos, muitas vezes sem todas as medidas de segurança necessárias ou a orientação adequada para os funcionários.

De fato, os cibercriminosos foram rápidos em explorar a incerteza e a vulnerabilidade dos usuários desavisados. Tentativas de *phishing* e outros golpes de engenharia social proliferaram, aproveitando a necessidade global de informações relacionadas à pandemia e ao uso maciço de ferramentas como aplicativos de videoconferência. Em abril de 2020, a Google relatou mais de dezoito milhões de e-mails diários de *malware* e *phishing* relacionados à COVID-19 em apenas uma semana. Os *hackers* enviaram e-mails de *phishing* se passando pela Organização Mundial da Saúde (OMS) e espalharam maciçamente links maliciosos para falsas reuniões de videoconferência e anexos contendo *malware*. Além disso, o Relatório de Segurança de 2021 da Check Point mostrou que, durante os primeiros meses de 2020, foram detectadas quase um milhão de tentativas de ataque por dia contra conexões de protocolo de área de trabalho

remota (RDP), amplamente utilizado entre as organizações para conexões remotas de funcionários. De fato, os ataques ao RDP foram a forma mais popular de ciberataque, superando até mesmo os e-mails de *phishing*. Durante a segunda metade do ano, à medida que mais organizações reforçavam a segurança de suas plataformas remotas, os *hackers* concentraram seus esforços na exploração das vulnerabilidades dos ativos privados dos funcionários e dos dispositivos de acesso remoto para penetrar em suas organizações. Embora essas ameaças tenham sido maximizadas por esse contexto global, elas não são novas e não desaparecerão: as pessoas continuam a viver em ambientes de alto risco, o que é especialmente grave em regiões do mundo onde as políticas e a tecnologia de cibersegurança são menos desenvolvidas e onde faltam educação e conscientização pública sobre o assunto. Em outras palavras, embora as mudanças provocadas pela pandemia da COVID-19 acabem se consolidando, elas destacaram a necessidade urgente de fortalecer as proteções individuais e coletivas contra os riscos cibernéticos.

O fortalecimento da cibersegurança é essencial para proteger os direitos dos cidadãos na esfera digital, como a privacidade e a propriedade, para promover a confiança das pessoas nas tecnologias digitais e apoiar o crescimento econômico por meio de uma transformação digital segura. Em especial, os cidadãos precisam ter certeza de que os sis-

temas digitais que usam para suas atividades pessoais ou profissionais, e também aqueles que envolvem seus dados pessoais, tenham medidas de segurança adequadas para garantir a integridade, a confidencialidade e a disponibilidade de suas informações e dos serviços dos quais dependem. Além disso, as violações de cibersegurança têm um impacto econômico significativo. Um relatório recente da McAfee avaliou que o cibercrime custa à economia global cerca de US\$ 600 bilhões por ano, ou 0,8% do produto interno bruto (PIB) global.

Israel, líder global em cibersegurança

O ecossistema de inovação e empreendedorismo de Israel é reconhecido mundialmente como um dos mais ativos do mundo, o que lhe valeu o nome de *Startup Nation*. De acordo com os indicadores de ciência e tecnologia da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), de março de 2021, Israel é o país da OCDE que investe a maior porcentagem de seu PIB (4,9%) em pesquisa e desenvolvimento (P&D). O país tem mais de trezentos centros de inovação, pesquisa e desenvolvimento de empresas multinacionais; desses, dezenas são dedicados à cibersegurança.

Não é surpresa, portanto, que 40% do investimento privado global em cibersegurança ocorra em Israel, que também tem o segundo maior ecossistema privado de cibersegurança do mundo, depois dos Estados Unidos. De acordo com dados de 2021, durante esse ano, US\$ 8,8 bilhões foram investidos em cerca de 131 empresas israelenses do setor, e mais de quarenta foram adquiridas por um total de US\$ 3,5 bilhões. O país tem mais de quinhentas startups de cibersegurança e, em 2021, 33% da população mundial de “unicórnios” eram israelenses. No total, sua exportação de produtos de cibersegurança até 2020 foi avaliada em US\$ 6,85 bilhões.

A Diretoria Cibernética Nacional de Israel (INCD, da sigla em inglês) é responsável por proteger o ciberespaço nacional e por estabelecer e promover a resiliência cibernética no país. A INCD opera em nível nacional para aumentar constantemente o nível de segurança das organizações e dos cidadãos, prevenir e gerenciar os ciberataques e fortalecer os recursos de resposta em caso de emergência cibernética. Sua posição como parte do gabinete do primeiro-ministro demonstra claramente a centralidade e a importância de suas competências para o país. Seus objetivos também incluem preparar e capacitar o setor privado israelense e o público em geral para que se protejam contra as ameaças cibernéticas, adotando tecnologias seguras, publicando práticas recomendadas, treinando pessoal e aumentando a conscientização. Também

é responsável por estabelecer e fortalecer a base científica e tecnológica da cibersegurança por meio do desenvolvimento de capital humano altamente qualificado, do apoio a pesquisas acadêmicas de ponta, do envolvimento em P&D tecnológico avançado e da promoção da indústria cibernética. A INCD dedica-se a manter um ciberespaço seguro, protegido e aberto para todos os habitantes e empresas do Estado de Israel e a facilitar seu crescimento e sua base científica e industrial.

Qual é a situação da cibersegurança na região da América Latina e do Caribe?

O Banco Interamericano de Desenvolvimento (BID) realiza regularmente estudos sobre a evolução da capacidade de seus Estados membros de se defenderem contra as crescentes ameaças no ciberespaço. O relatório regional de maturidade da cibersegurança 2020, *Cibersegurança: Riscos, Progresso e o Caminho a Seguir na América Latina e no Caribe*, preparado em colaboração com a Organização dos Estados Americanos (OEA), mostrou que os países estavam em diferentes estágios de desenvolvimento em sua preparação para enfrentar os desafios da cibersegurança, mas, em geral, ainda tinham muito espaço para melhorias.

Enquanto em 2016, ano da primeira edição do relatório, 80% dos países da região não tinham uma estratégia nacional de cibersegurança, esse número caiu para 60% até 2020. Além disso, apenas alguns países controlam a exposição de suas infraestruturas essenciais – como energia, saúde, telecomunicações, transporte, abastecimento de água e finanças – a ciberataques. Como revela o Relatório de 2020, apenas sete dos 32 países avaliados tinham um plano de proteção cibernética de infraestruturas críticas. Essa é uma das descobertas mais preocupantes, considerando o impacto catastrófico que os ataques a esses setores podem ter não apenas nas economias nacionais, mas na vida de todos os seus cidadãos.

Com relação à capacidade dos países de gerenciar e responder a incidentes de cibersegurança, o mesmo estudo constatou que 63% dos países tinham equipes de resposta a incidentes de segurança, como Equipes de Resposta a Emergências Informáticas (CERTs, da sigla em inglês) ou Equipes de Resposta a Incidentes de Segurança em Computadores (CSIRTs, da sigla em inglês). No entanto, dos vinte países que tinham essas equipes, apenas três haviam alcançado maturidade avançada em sua capacidade de coordenar essas respostas. Na verdade, 23 dos 32 países ainda estavam em um estágio inicial de maturidade nessa área. Essa constatação chamou a atenção para a necessidade de os países reforçarem a capacidade de suas equipes de coordenar efetivamente suas respostas a in-

cidentes cibernéticos. Além disso, o relatório examinou a disponibilidade de oportunidades educacionais e de treinamento em cibersegurança e constatou que menos da metade dos países da região oferecia educação formal em cibersegurança, como pós-graduação, mestrado ou cursos técnicos. Não é preciso dizer que ter profissionais treinados em número suficiente é essencial para projetar e implementar as políticas e medidas de cibersegurança necessárias para garantir a resiliência de um país diante de ciberataques cada vez mais sofisticados e complexos.

O que o BID está fazendo para apoiar a região?

Nos últimos anos, o BID tem apoiado ativamente a região na capacitação em cibersegurança, no projeto e na implementação de uma política pública nacional de cibersegurança e no fortalecimento das capacidades setoriais nessa área. Esse apoio é realizado de várias formas. O BID disponibilizou assistência financeira no valor de dezenas de milhões de dólares para que os países da América Latina e do Caribe (ALC) desenvolvessem capacidades nacionais de cibersegurança por meio de mais de quinze operações de investimento no setor público, além de um financiamento adicional significativo para garantir a cibersegurança em projetos de investimento em transformação digital.

Também fornece orientação técnica e realiza projetos de cibersegurança em toda a região na forma de consultorias, diagnósticos e projetos personalizados de fortalecimento da cibersegurança, em tópicos que incluem a proteção cibernética de infraestruturas críticas, cibercrimes e perícia, projeto e fortalecimento de CSIRTs e Centros de Operações de Segurança (SOCs, da sigla em inglês), e estratégias nacionais e setoriais de cibersegurança. Além disso, o BID tem feito esforços significativos para oferecer oportunidades para que os profissionais da ALC fortaleçam e atualizem suas habilidades nesse campo, oferecendo regularmente workshops e atividades de treinamento. Isso incluiu cursos executivos de duas semanas sobre cibersegurança, oferecidos em conjunto com a Universidade Hebraica de Jerusalém, em Israel, além de cursos personalizados sobre proteção de infraestrutura crítica e outros voltados para setores específicos. Por fim, o BID produziu várias publicações de alto impacto sobre questões de cibersegurança nacionais e setoriais e continua a atualizar e expandir regularmente esse conjunto de conhecimentos.¹

O BID e a INCD: unindo forças

Os desafios da cibersegurança, assim como os da própria internet, são de natureza global, portanto, o compartilhamento de conhecimentos e ferramentas para enfrentá-los beneficia a população como um todo. Reconhecendo essa realidade, a INCD e o BID fizeram uma parceria para disponibilizar a experiência israelense para os países da ALC. A colaboração entre as duas instituições forneceu forte apoio à região na forma de treinamentos executivos e técnicos sobre tópicos avançados de cibersegurança, conferências de ponta para funcionários do governo da ALC e profissionais da área, além de projetos inovadores de assistência técnica. A presente publicação é mais um produto dessa colaboração, consistindo em uma série de guias metodológicos de cibersegurança para organizações, desenvolvidos pela INCD à luz da análise de riscos, dos métodos de ataque, incidentes cibernéticos e padrões globalmente aceitos. Esses guias foram traduzidos para o espanhol e o inglês, em uma atividade conjunta das duas organizações, com o objetivo de permitir o acesso a esse acervo de conhecimento por parte do público da região da ALC e, assim, contribuir para aumentar sua resiliência cibernética.

Essa coleção oferece orientação prática sobre uma série de questões metodológicas e técnicas relevantes para o fortalecimento

da cibersegurança em organizações de todos os tipos, com base nos padrões globais mais reconhecidos.

O desafio de proteger o espaço digital continuará a crescer, assim como a necessidade de especialização comprovada para enfrentá-lo. As reflexões contidas neste documento têm o objetivo de servir como recurso para aprimorar o tão necessário treinamento profissional em cibersegurança observado atualmente na ALC. Esses guias ajudarão a elevar os padrões organizacionais, promoverão mais conscientização e cultura de cibersegurança nas organi-

zações e no público em geral, e informarão os tomadores de decisão, gerentes e líderes em suas iniciativas de cibersegurança. Estamos confiantes de que esses guias servirão como um roteiro para profissionais e líderes da ALC, trabalhando juntos para construir um futuro mais seguro e próspero.



1. Consulte o site do Grupo de Dados e Governo Digital (DDG, do inglês) da divisão de Inovação para Servir ao Cidadão (ICS, do inglês) do BID, disponível em: <https://www.iadb.org/en/who-we-are/topics/reformmodernization-state/data-and-digital-government>.

Sumário executivo

O objetivo da Metodologia de Defesa Cibernética é fornecer à economia israelense um método profissional ordenado para lidar com riscos cibernéticos na organização. Adotando o método apresentado neste documento, a organização reconhecerá os riscos relevantes, formulará uma resposta de defesa e implementará o devido plano de redução de riscos.

Etapa A. Identificação da categoria à qual a organização pertence

Categoria A: organizações com potencial médio a baixo de sofrer danos em decorrência de um ciberincidente.

Categoria B: organizações com potencial alto de sofrer danos em decorrência de um ciberincidente.

Um questionário de categorização é fornecido na página 19.

Etapa B. Realização de um processo de avaliação e gestão de riscos

As atividades de defesa cibernética são realizadas devido ao desejo da organização de gerenciar os riscos cibernéticos aos quais está exposta.

Para isso, primeiramente, a organização define quais são seus principais **objetivos de defesa** (geralmente, processos empresariais ou ativos digitais), qual nível de defesa é necessário e quais são as lacunas de defesa em comparação com a situação desejada; em seguida, formula um plano de ação para minimizar as lacunas.

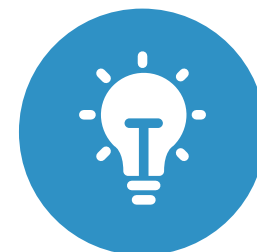
Cada organização tem sua forma de executar esse processo, dependendo do porte, conformidade com os requisitos legais e regulatórios, e outros parâmetros.

Este documento apresenta diversos métodos de avaliação e gestão de riscos, distinguindo entre organizações com um potencial relativamente pequeno de sofrer danos (até US\$ 1,5 milhão) e organizações com um potencial maior de sofrer danos, para as quais uma metodologia ampliada foi desenvolvida.

Produto final após a aplicação deste documento

A organização precisa entender o mapa de riscos organizacionais e quais controles são necessários para reduzir esses riscos, incluindo as prioridades certas para implementar o plano de trabalho.

Esses controles formarão as bases para a elaboração do plano de trabalho, devidamente alocando recursos e preparando a organização.



/01. Introdução

O ciberespaço é uma parte integrante do nosso cotidiano. No âmbito pessoal, pesquisamos informações na internet, percorremos os nossos trajetos com a ajuda de programas de navegação, conversamos ao telefone, e alguns de nós têm até um marca-passo ou uma bomba de insulina conectada à internet, e tudo isso faz parte do ciberespaço. No âmbito comercial, usamos cartões de crédito, gerenciamos bancos de dados de clientes, gerenciamos organizações internacionais por meio de redes de computador, comercializamos, compramos e vendemos, tudo isso graças ao ciberespaço.

Para muitos de nós, um ciberespaço disponível, acessível e confiável é uma condição necessária para lidarmos com o cotidiano, principalmente na esfera empresarial. Isso é fácil de entender quando perdemos tudo isso temporariamente. Como gerenciamos uma empresa sem um celular? Sem o conhecimento armazenado na rede corporativa? Sem a capacidade de liquidar operações com cartão de crédito?

No ciberespaço, há opções e oportunidades por um lado, mas ameaças e riscos por outro. No domínio cibernético, atividades de espionagem do Estado, espionagem industrial, crime organizado e crimes ocasionais são comuns. Tudo isso pode afetar a segurança nacional (por exemplo, causando danos à infraestrutura nacional essencial, como os sistemas de eletricidade ou água, por meio do ciberespaço) ou a gestão empresarial

(por exemplo, por meio de espionagem comercial ou chantagem econômica).

Atualmente, cada organização tem uma forma diferente de proteger-se dessas ameaças. Existem muitas informações na internet sobre formas de proteger-se contra os riscos cibernéticos, consistindo em uma coletânea de metodologias ordenadas, boas práticas, o que fazer e não fazer, e muito mais.

Muitas organizações em Israel e no mundo todo deparam-se com dúvidas como: “Estamos investindo o suficiente em defesa cibernética?”, “Estamos investindo adequadamente em defesa cibernética?” ou “Estamos investindo em defesa cibernética de acordo com as práticas comuns na nossa economia ou setor?”.

A Metodologia de Defesa Cibernética apresentada neste documento ajudará as organizações a mapear os riscos cibernéticos, entender a importância organizacional da concretização dos riscos e definir proteções proporcionais para mitigar os principais riscos.

A Metodologia é acompanhada por vários auxílios que ajudarão a organização a adotá-la com facilidade. Esses auxílios incluem complementos profissionais, procedimentos e recomendações de implementação da defesa cibernética para diversas áreas, procedimentos aplicáveis com base nas leis e regulamentos israelenses, bem como na

padronização internacional, informatização da Metodologia por meio de uma plataforma tecnológica conveniente, e muito mais.

Todas as informações mais recentes são publicadas no site da Diretoria Cibernética Nacional de Israel: https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page



/02. Princípios da Metodologia de Defesa Cibernética

O maior princípio da Metodologia de Defesa Cibernética é a defesa contra ameaças relevantes, ou seja, reconhecer que, quando se trata de proteger a continuidade das operações da organização, seus ativos e seus objetivos, ela deve se basear no entendimento da ameaça referencial e nas informações e tendências em constante mudança do campo em questão. Esse princípio divide-se nos subprincípios a seguir.



01

Responsabilidade da administração: a responsabilidade pela proteção das informações cabe, acima de tudo, à administração da organização.

02

Defesa da perspectiva do adversário: o peso das recomendações de defesa e a definição de prioridades para sua implementação advêm diretamente do entendimento dos casos de ataque comuns e da eficácia das recomendações de defesa nesses casos. A resiliência organizacional é conquistada com base nas recomendações de defesa, de acordo com as ameaças e as formas de agir específicas da organização.

03

Defesa baseada no conhecimento e na experiência de Israel: a Metodologia de Defesa Cibernética permite manter o foco nos riscos relevantes para cada organização. Como parte das atividades da Diretoria Cibernética Nacional de Israel, auditorias e avaliações de informações periódicas são realizadas em

todas as áreas da economia israelense. Essas ações permitem priorizar organizações em setores específicos dentro da área de defesa.

04

Defesa de acordo com o potencial de sofrer dano: o investimento na proteção de cada alvo de defesa na organização dependerá de quão crucial o alvo é para o funcionamento da organização.

05

Defesa baseada na profundidade da implementação: a Metodologia de Defesa Cibernética permite que a organização implemente controles com diferentes graus de maturidade em áreas como centros de operações de segurança, prevenção de perda de dados ou pesquisas de risco. Assim, em vez de considerar os controles exclusivamente do ponto de vista da conformidade, a organização examina-os de acordo com a eficácia de sua implementação. Isso se reflete devidamente na definição de “profundidade da implementação” de cada recomendação de defesa (controle) e na definição de “indícios necessários”.

/03. Estrutura da Metodologia de Defesa Cibernética

A Metodologia consiste em duas faixas separadas de avaliação e gestão de riscos, derivadas principalmente dos danos em potencial que a organização pode sofrer em decorrência de um ciberincidente, como nos casos a seguir.

01

Faixa das organizações da categoria A: projetada para organizações cujo alcance dos danos sofridos no caso de um ciberincidente não excede US\$ 1,5 milhão. Esta faixa inclui um processo simples e rápido de mapeamento dos objetivos de defesa e a resposta a uma quantidade limitada de perguntas elaboradas sob medida para organizações desta categoria. Geralmente, o processo é realizado por uma parte externa que acompanha os aspectos de defesa cibernética da organização.

02

Faixa das organizações da categoria B: projetada para organizações cujo alcance dos danos sofridos no caso de um ciberincidente pode exceder US\$ 1,5 milhão. Esta faixa inclui um processo de avaliação de riscos, entendendo-se a resposta de defesa necessária à matriz de riscos e ao apetite de risco, examinando-se a situação atual em contraste com as recomendações de defesa aceitas pelo setor (análise de lacunas) e formulando-se um plano de trabalho para mitigar os riscos (plano de mitigação) ou outras medidas para abordar os riscos. Na maioria dos casos, o processo de avaliação e a implementação de suas conclusões são liderados por um indivíduo responsável pela defesa cibernética dentro da organização (devido à posição que ocupa ou às suas responsabilida-

Para verificar se um ciberincidente na sua organização pode causar danos acima de US\$ 1,5 milhão, recomendamos que considere os seguintes parâmetros, entre outros:

- perda de renda em decorrência de uma interrupção da continuidade operacional;
- o custo de tratar o incidente (incluindo equipes de resposta, especialistas em conteúdo e mais);
- o custo de recuperar totalmente os sistemas de informação (incluindo licenças, equipamentos e programas);
- custo direto decorrente de uma violação das leis/regulamentos e sinistros empresariais;
- danos indiretos, como danos à reputação, incluindo o impacto na perda de clientes existentes e novos.



des além de sua posição). Às vezes, uma parte externa é contratada para isso.

A fim de avaliar os danos com mais precisão, é possível utilizar calculadoras e estudos profissionais que levem em consideração parâmetros como o setor no qual a organização atua, o tipo de informação e a quantidade de registros mantidos pela organização.

No entanto, a organização precisa examinar o potencial de sofrer danos através de uma lente mais ampla que envolva aspectos da responsabilidade corporativa. O conceito por trás dessa abordagem é o de que a essência da organização comercial é, além de gerar lucro para os acionistas, agregar valor para todas as partes

interessadas: clientes, funcionários, fornecedores, investidores, a comunidade e o meio ambiente.

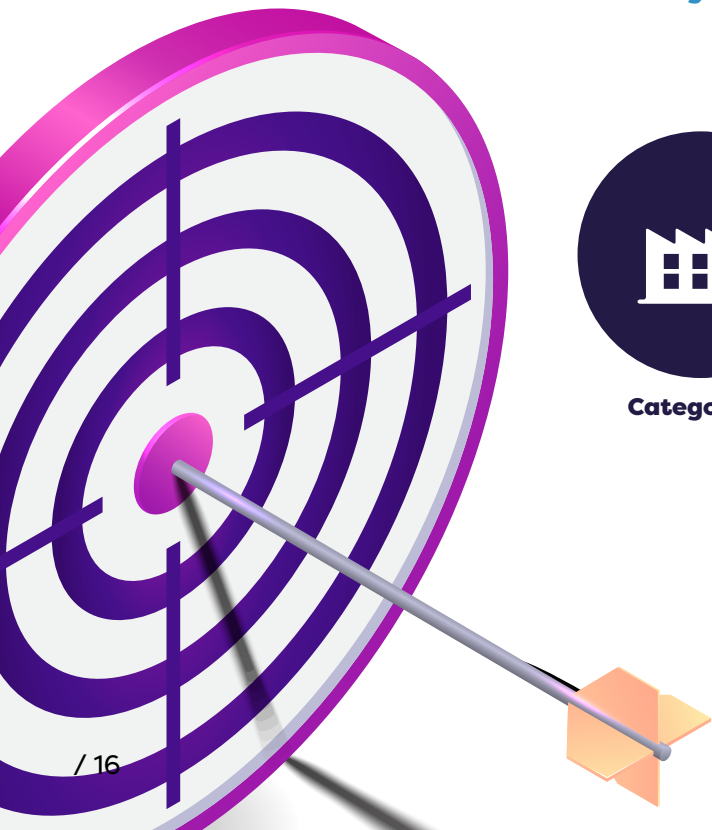
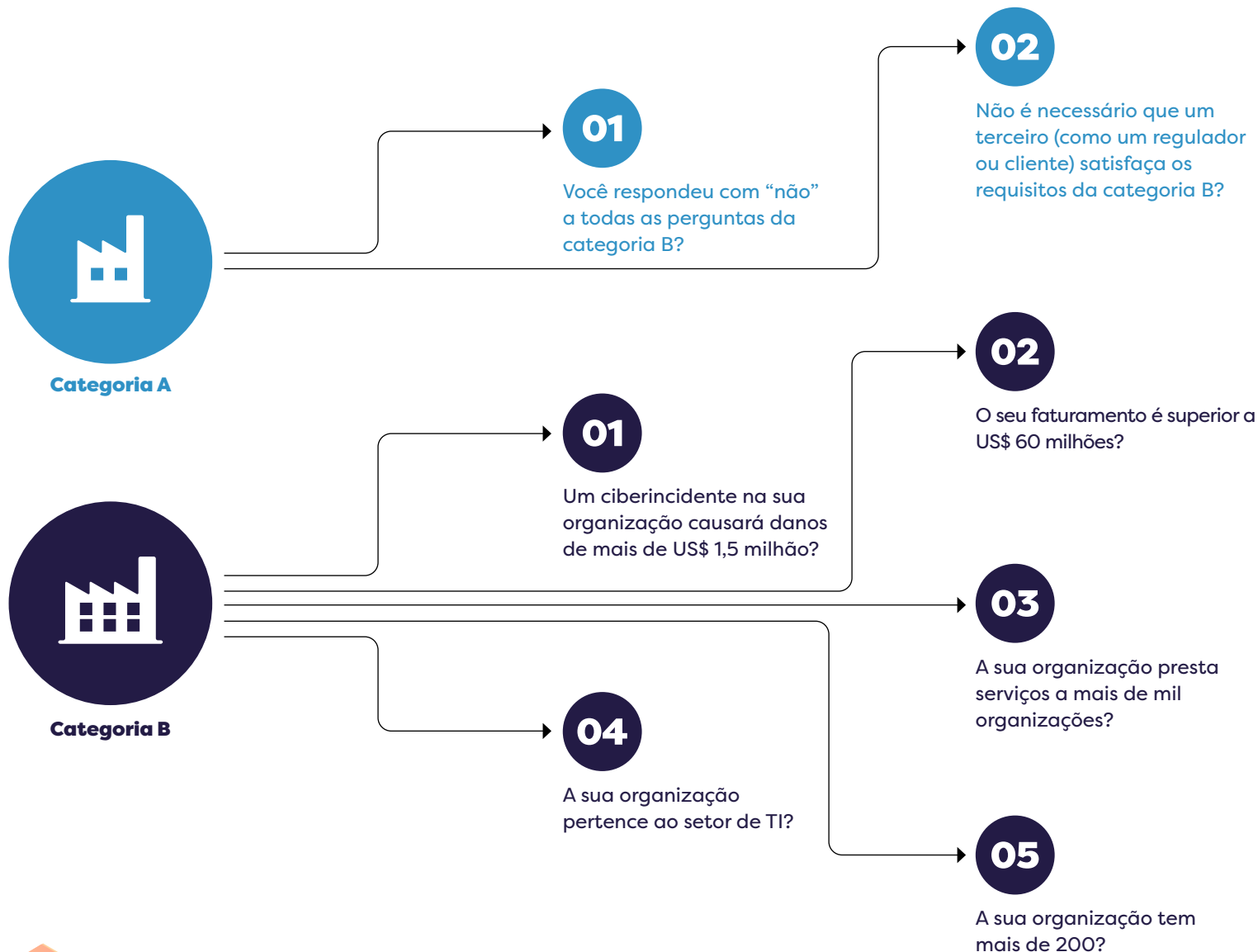
A adoção dessa abordagem mede os efeitos de um ciberincidente nas partes interessadas da organização, fortalece a confiança mútua entre elas e a organização, e aumenta o desempenho econômico no longo prazo. Essa abordagem inclui os danos em potencial à vida humana, à confiança do público e a terceiros, bem como uma visão ampla e abrangente dos danos agregados tanto à organização quanto às esferas de influência mais amplas.

Para entender rapidamente a qual categoria a sua organização pertence, você pode usar as regras gerais a seguir.

Árvore de classificação organizacional

O Gráfico 1 mede alguns parâmetros, como o porte da organização, a quantidade de clientes, o faturamento e a dependência de tecnologias digitais. Esta árvore não substitui a avaliação do potencial de sofrer danos, mas pode ajudar a colocar a organização no rumo certo.

Gráfico 1. Árvore de classificação organizacional



Organizações representativas em cada categoria

A Tabela 1 apresenta um exemplo geral de uma possível divisão de tipos de organização nas categorias recomendadas. A divisão acima é simplista e tem como objetivo fornecer uma regra preliminar geral para classificar as organizações em diferentes categorias.

Tabela 1. Tipos de organização nas categorias recomendadas

Categoria A	Categoria B
Firma de advocacia de pequeno porte	Município
Firma de contabilidade de pequeno porte	Hospital
Gráfica de pequeno porte	Instituição acadêmica
Empresa de tradução de documentos de pequeno porte	Ministério do governo
Fábrica de pequeno porte	Empresa de software
	Prestador de serviços de informática

Questionário

Responder às seguintes perguntas ajudará a decidir a qual categoria a organização pertence.

Qual é a motivação para atacar a organização?

- Que tipos de informação existem na organização? Por exemplo, informações pessoais, dados financeiros (como informações de crédito), informações médicas, informações de patentes ou segurança.
- Qual é o escopo das informações sensíveis disponíveis na organização? Por exemplo, existem centenas, milhares ou centenas de milhares de registros?
- Qual é a natureza da organização? Por exemplo, é uma empresa de software que pode fornecer um caminho de penetração para um agressor em potencial? É uma organização que armazena informações de vários clientes? Ou é uma organização considerada um símbolo nacional?

Qual é a superfície de ataque da organização?

Por exemplo, a quantidade de interfaces abertas da organização e seu tipo, a implantação e acessibilidade globais dos ativos

digitais da organização, ou a quantidade de fornecedores da organização e seu tipo.

Que recursos a organização dedica à defesa cibernética?

Por exemplo, a organização conta com um Diretor de Segurança da Informação (CISO, na sigla em inglês)? O Gerente de Sistemas de Informação dedica recursos à defesa cibernética? Ou o orçamento de defesa cibernética da organização é compatível com as ameaças existentes no setor? A administração definiu-o como uma certa porcentagem do faturamento anual ou do orçamento de TI?

Se a organização assumir obrigações adicionais por força da lei e/ou da regulamentação a ser cumprida, de requisitos contratuais ou necessidades comerciais diversas, isso pode resultar em sua transferência da categoria A para a categoria B. Além disso, organizações altamente dependentes da tecnologia que possam sofrer danos consideráveis em decorrência de um ciberincidente devem considerar realizar o processo de acordo com os requisitos da categoria B.

/04.

Processo de planejamento através da lente da organização

Aplicação deste documento conforme a categoria da organização.



Para uma organização da categoria A

Gráfico 2. Processo de planejamento para uma organização da categoria A



Para uma organização de categoria B

Gráfico 3. Processo de planejamento para uma organização da categoria B



Implementação da Metodologia de Defesa Cibernética em uma organização da categoria A

Estágio 1: mapeamento da atividade

Consultar a equipe de suporte técnico para saber quais são os tipos de equipamento e ativos de informática usados pela organização. Entender quais são os ativos digitais da orga-

nização e onde estão armazenados. O propósito deste estágio é entender as metas de defesa contra ciberameaças. Como parte do estágio de demarcação, é necessário entender se a organização possui bancos de dados, ativos digitais, como redes sociais, ou sistemas e softwares organizacionais, como sistemas de folha de pagamento, sistemas de presença ou estações de pagamento e liberação.

No fim deste estágio, a organização contará com uma lista de ativos cujo nível de defesa deve ser contrastado com os riscos cibernéticos de acordo com a lista de controles recomendados.

Gráfico 4. Exemplo de mapeamento dos objetivos de defesa em uma organização da categoria A



Estágios 2 e 3: avaliação dos riscos e determinação de uma estratégia para abordá-los. Os Dez Mandamentos para uma organização da categoria A

Uma organização da categoria A precisa defender-se à altura do potencial de sofrer danos. Portanto, ela precisa adotar controles extremamente eficientes.

Em muitos ciberincidentes, os agressores não consideram o porte da organização ou o potencial de danos que ela pode sofrer. Muitas pequenas empresas já sofreram ataques de *ransomware*, vazamentos de bancos de dados de clientes, furtos de informações de clientes, entre outros.

A fim de reduzir a chance de sofrer danos nesses tipos de incidente e aumentar a capacidade de sobreviver e dar continuidade aos negócios no caso de um ataque, recomenda-se que cada organização adote os requisitos de defesa horizontal apresentados no Apêndice A deste documento. Esses controles dividem-se nas seguintes dez categorias de defesa apresentadas na Tabela 2.



Tabela 2. Dez categorias de proteção para organizações da categoria A

1. Responsabilidade da administração: entender os riscos para a organização que existem no ciberespaço e formular um plano de trabalho para fechar as lacunas de defesa nesta área.

2. Prevenção de código malicioso: utilizar tecnologias de tratamento de *malware* e atualizar a segurança dos sistemas da organização. Em particular, é necessário tomar precauções contra *malware* enviado por e-mail e ao navegar por sites.

3. Criptografia: criptografar a conexão remota dos funcionários e fornecedores da organização, utilizando mecanismos de criptografia simples e comerciais. Criptografar o acesso às informações sensíveis, utilizando um meio de comunicação criptografado (para navegar tanto pelo site da organização a partir de uma rede sem fio doméstica quanto por sites de clientes e fornecedores a partir da organização).

4. Computação em nuvem e aquisição de softwares: assinar um contrato com o fornecedor que exija conformidade com as normas aceitas de defesa de softwares e das informações, como a metodologia da cadeia de suprimentos da Diretoria Cibernética. Em particular, ao carregar algo para a nuvem, é necessário assegurar a divisão da responsabilidade pela defesa cibernética entre o provedor de nuvem e a organização.

5. Defesa das informações: definir mecanismos de defesa para controlar como as informações saem da organização.

6. Defesa dos computadores e periféricos: definir o nível de defesa necessário para os computadores. Este nível inclui a alteração de senhas padrão, a remoção de softwares desnecessários, o fortalecimento das interfaces externas e a exclusão de contas de usuários não essenciais.

7. Recursos Humanos: orientar os funcionários assim que contratados, conscientizá-los e pedir-lhes que assinem um acordo de não divulgação das informações da organização após o término do vínculo empregatício. Definir políticas relativas ao uso de equipamentos de informática privados e sua conexão com a organização, e formular práticas profissionais relativas a redes e computadores. Definir políticas para as equipes de computação e defesa cibernética (e averiguar se os funcionários são internos ou externos), incluindo conscientização e controle de suas atividades.

8. Documentação e monitoramento: para investigações/análises futuras, monitorar e documentar ações incomuns que a organização queira saber se ocorreram e que indiquem uma ciberameaça.

9. Segurança da rede: certificar-se de que o acesso à rede esteja sob o controle da organização (fornecedores e funcionários não podem se conectar remotamente à rede quando e como quiserem) e de que a rede esteja preparada para ataques de negação de serviço. Em particular, a área de exposição precisa ser reduzida, devendo-se analisar se a organização está exposta ao resto do mundo devido a interfaces desnecessárias e/ou desprotegidas.

10. Continuidade dos negócios: garantir a capacidade de recuperação em casos de queda de sites, exclusão de informações ou bloqueio de arquivos. Em particular, deve haver um back-up eficaz. Uma restauração inicial deve ser realizada periodicamente, e a frequência e o tipo de back-up necessários devem ser definidos.

Após analisar o progresso da implementação dos controles, deve-se decidir qual é a resposta necessária aos riscos decorrentes das lacunas na implementação desses controles.

Muitas vezes, esses riscos dividem-se em violações da confidencialidade dos dados, continuidade dos negócios e integridade das informações. Esses riscos podem ter diversas consequências, como danos à reputação da empresa; impossibilidade de receber clientes e prestar-lhes serviços; exposição a sinistros decorrentes de violações da legislação e/ou dos regulamentos; ou vazamento de informações dos clientes, que podem vir a processar a organização. Esses riscos precisam ser contrastados com os objetivos de defesa definidos no Estágio 1.

Estágio 4: formulação de um plano de trabalho

Após a organização definir os riscos para seus objetivos de defesa, um plano anual deverá ser formulado para reduzir e/ou transferir esses riscos, de acordo com a decisão tomada no Estágio 3 acima. Esse plano poderá incluir

a implementação de processos e a aquisição de soluções, como: inspeção periódica dos back-ups da empresa, proteção de laptops, instalação de software de proteção nas estações de trabalho e treinamento dos funcionários da organização.

Durante a formulação do plano de trabalho para fechar as lacunas de controle, os fatores a seguir precisam ser levados em consideração.

01

Eficácia do controle: como ele contribui para reduzir o risco para a organização.

02

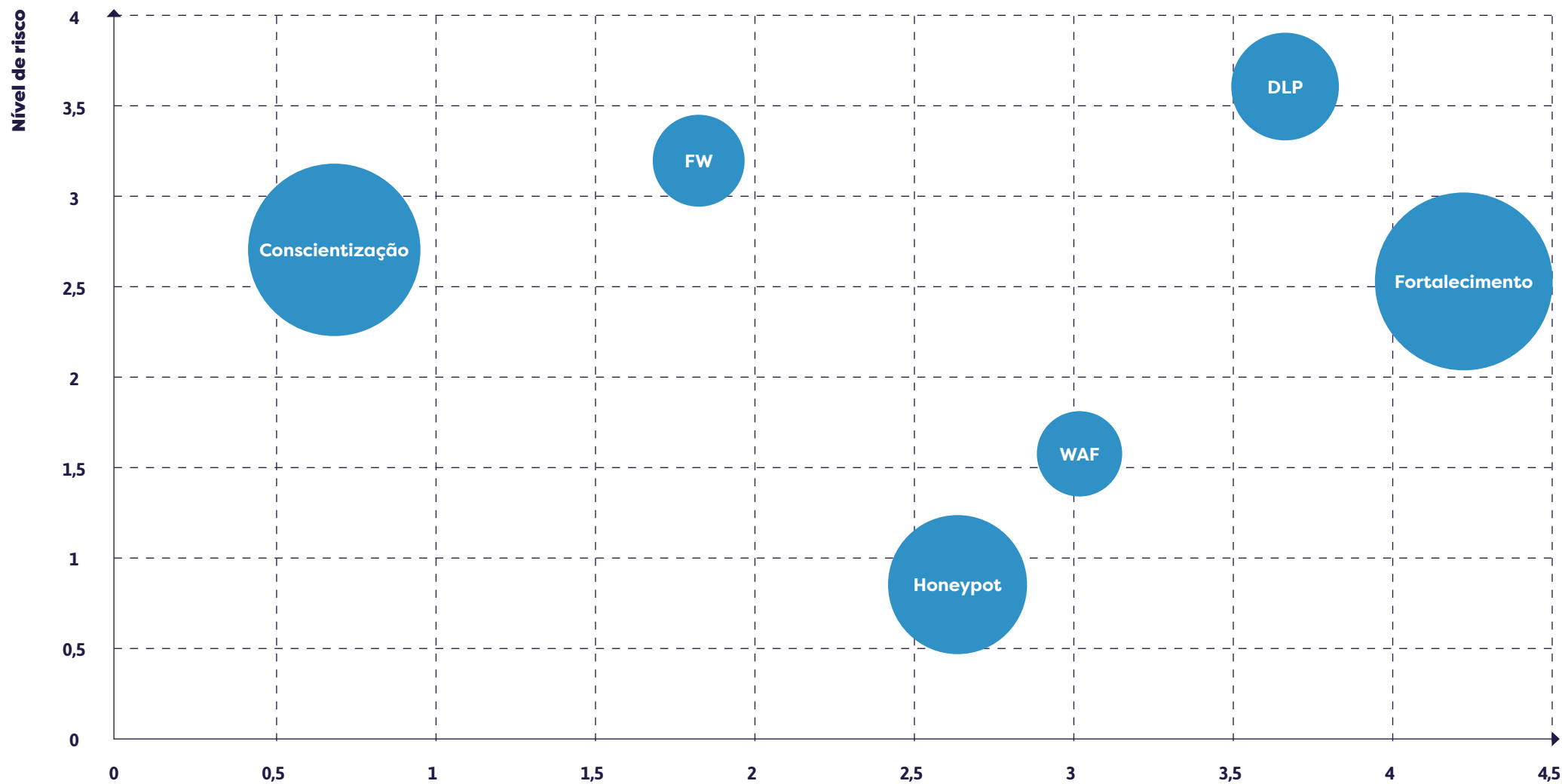
Custo de realização da solução: representado abaixo pelo eixo de “custo da solução” (duração da implementação, complexidade da implementação, força de trabalho e equipamentos necessários).

03

Velocidade de aplicação: representada abaixo pelo tamanho do círculo.

Gráfico 5. Exemplo de ponderação de parâmetros para determinar a prioridade do plano de trabalho para uma organização da categoria A

Observação: FW: firewall; WAF: firewall de aplicativo da web;
DLP: prevenção contra perda de dados.



O nível de risco do ativo: o eixo y no exemplo acima.

O custo de implementação da solução: o eixo x no exemplo acima.

Velocidade da aplicação da solução: representada pelo tamanho do círculo no exemplo acima.

Custo de implementação da solução

Tabela 3. Suporte para preencher os dados do plano de trabalho

Alvos de defesa mapeados na organização	Como: site, banco de dados de clientes, estações de trabalho, servidor de e-mail, servidor de back-up, etc.			
A família de controles	Existe/não existe	Eficácia do controle	Custo de realização	Ponderação/priorização de dados
Responsabilidade da administração				
Prevenção de código malicioso				
Criptografia				
Computação em nuvem e aquisição de softwares				
Proteção das informações				
Defesa dos computadores				
Recursos Humanos				
Documentação e monitoramento				
Segurança da rede				
Continuidade dos negócios				

Apresentamos uma tabela auxiliar para preenchimento dos dados. O plano de trabalho proposto será aprovado pelo diretor da organização.

Estágio 5: auditoria e controle contínuos

O ritmo de implementação do plano de trabalho e sua relevância devem ser avaliados periodicamente. A finalidade deste estágio é verificar se há novos ativos de informação, quais controles foram implementados até o momento e quais recursos e opiniões da administração da organização sobre o assunto são necessários.

A auditoria pode ser realizada paralelamente a uma revisão periódica (por exemplo, anualmente ou bianualmente) ou com base nos ciberincidentes ocorridos nos últimos anos em pequenas empresas, tanto em Israel quanto no exterior. A auditoria ajudará a administração a focar seus esforços e priorizar os recursos de acordo com os riscos mais relevantes para a organização.

Uma organização da categoria A termina de ler este documento aqui.

Implementação da Metodologia de Defesa Cibernética em uma organização da categoria B

Estágio 0: governança corporativa e estratégia de gestão de riscos corporativos

Antes de identificar as ameaças e respostas na organização, a governança corporativa que apoia o processo (às vezes chamada de Sistema de Gestão da Segurança da Informação) precisa ser avaliada: sua finalidade, definição de hierarquia, funcionários, rotinas de defesa e procedimentos realizados. O objetivo é mapear os riscos cibernéticos e a resposta a esses riscos, bem como apresentar um aprimoramento contínuo.

Como parte da definição da governança corporativa, a organização **precisa abordar as questões a seguir.**

01

Quem é a parte/equipe/pessoa que realiza a avaliação de riscos dentro da organização? Quais são sua formação e sua experiência na

área? Que recursos estão disponíveis para isso? Que diretoria supervisiona isso dentro da organização?

02

Existe um mapeamento de processos sensíveis na organização como parte da Análise de Impacto nos Negócios, que pode ser usado na avaliação de riscos? Como a avaliação de riscos se insere nas metas da organização?

03

Que métodos serão usados para identificar novos riscos, e com que ferramentas a organização conta para identificá-los eficazmente?

04

Com que frequência a avaliação de riscos é realizada? A avaliação de riscos será realizada com base em casos reais de ataque e atribuição de ameaças, ou de acordo com a metodologia geral de gestão de riscos da organização?

05

Quem tem autorização para decidir correr um risco? Quem tem autorização para aprovar a atividade de redução de riscos? Quem tem autorização para atualizar o risco, reduzindo seu valor, com base na implementação dos controles de defesa e na atividade de correção/compensação?

06

Existe um comitê de direção para Defesa Cibernética e das Informações? Em caso afirmativo, quem são os membros? Existe um comitê de direção para a questão da continuidade dos negócios? Em caso afirmativo, quem são os membros?

Estágio 1: demarcação da atividade e pesquisa de avaliação de riscos

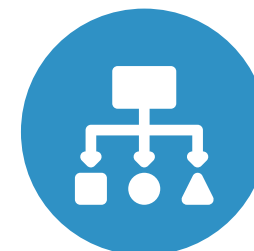
A demarcação dos objetivos de defesa é uma etapa inicial necessária para entender o ambiente de atuação da organização e definir os limites do setor e das áreas de responsabilidade. **Neste estágio, a organização definirá, entre outros, os temas a seguir.**

01

Os limites da demarcação entre o Diretor de Segurança da Informação (CISO) e outros funcionários da organização: a divisão de autoridade e de responsabilidades com as partes interessadas internas, como o Diretor de Segurança, o Gerente de Operações, o Gerente de Sistemas de Informação, o Gerente de Riscos, o Assessor Jurídico e o Diretor Executivo. Se a organização precisar de serviços cibernéticos e/ou de computação como um serviço (provedores de serviços de segurança gerenciados), é importante definir a interação e a divisão de responsabilidades entre as partes.

02

Conhecimento aprofundado da estratégia da organização (incluindo a visão, os objetivos, as características do mercado comercial e a concorrência) e como a questão da Defesa Cibernética e das Informações se encaixa nela.



03

Qual é a demarcação da pesquisa de riscos?

A pesquisa inclui aspectos como câmeras de segurança, sistema de ar condicionado, linha de produção e ambientes operacionais, dispositivos eletrônicos privados dos funcionários, cadeia de suprimentos e filiais no exterior?

No fim deste estágio, a organização contará com um documento que descreve seu ambiente comercial, suas características e a demarcação da atividade de pesquisa.

Esta etapa pode afetar os documentos de continuidade dos negócios, o plano de resposta a incidentes da organização, contratos com fornecedores, documentos da Análise de Impacto nos Negócios, processos de incorporação e aquisição, entre outros.

Estágio 2: avaliação de risco

Este estágio consiste em três subestágios: **identificação de riscos > análise de riscos > avaliação de riscos.**

Existem diversos métodos de avaliação de riscos, como FAIR, OCTAVE e ISO 27005. Cada um tem suas próprias características e vantagens. Este documento apresenta um método que combina muitas vantagens dos métodos conhecidos e adiciona o conhecimento oriundo de ex-

periências práticas no ramo, ajustando-o à economia israelense.

2.1 Identificação de riscos

Esta atividade consiste nas duas subetapas a seguir.

01

Mapeamento dos alvos de defesa: entender os alvos em potencial que a organização precisa proteger em termos cibernéticos. Esse mapeamento pode incluir uma lista de ativos, como aplicativos, redes ou sistemas operacionais. O mapeamento também pode incluir uma lista de processos comerciais importantes, associando os ativos digitais que apoiam esses processos (como um processo de folha de pagamento, geração de relatórios do mercado financeiro ou liberação de cartões de créditos). Recomenda-se dar mais prioridade ao mapeamento dos processos comerciais que ao mapeamento dos objetivos de defesa, analisando-se as diversas interações.

02

Atribuição de riscos e/ou ameaças e vulnerabilidades: após mapear os objetivos de defesa, as ciberameaças relevantes para os processos e ativos identificados devem ser analisadas. Por exemplo, qual é um possível plano

de ação por meio do qual um agressor pode concretizar a ameaça, como, por exemplo, interrompendo o processo de produção ou obtendo acesso ao banco de dados sensíveis da organização? O Apêndice B deste documento apresenta uma lista de ameaças e vulnerabilidades comuns.

A fim de realizar um mapeamento abrangente dos ativos de TI, recomenda-se obter uma lista de ativos do departamento de sistemas de informação da organização. Também é importante obter do departamento de aquisições uma lista de fornecedores de produtos

e serviços, o que pode permitir detectar sistemas fornecidos como um serviço que, às vezes, não são gerenciados pelo departamento de informática central da organização (“Shadow IT”). A fim de mapear os ativos de Tecnologia Operacional, recomenda-se organizar uma reunião com o Diretor de Operações e o Diretor de Segurança (principalmente em organizações industriais).

Uma organização que conta com um plano de continuidade dos negócios poderá usá-lo para mapear os processos comerciais materiais (utilizando a Análise de Impacto nos Negócios).

Resolução do mapeamento de alvos

O mapeamento dos alvos de defesa é um processo que exige tempo e recursos. Para realizar o processo eficazmente, deve-se levar em consideração a resolução do mapeamento.

Por exemplo: por um lado, é óbvio que não é necessário listar todos os servidores e estações de trabalho, mas, por outro, uma generalização por alto de todos os servidores no mesmo lugar pode resultar em custos de defesa desproporcionais (investimento excessivo ou insuficiente em contraste com o risco real).

Atenção: informações sensíveis da organização podem ser encontradas nas instalações dos fornecedores ou armazenadas na nuvem. Além disso, às vezes, informações sensíveis são armazenadas em um arquivo, não em um banco de dados ou sistema de informação exclusivo. Um bom mapeamento também engloba esses ativos. Uma visão geral dos principais processos de uma empresa é uma boa forma de certificar-se de que o mapeamento leve em consideração todos os ativos essenciais.

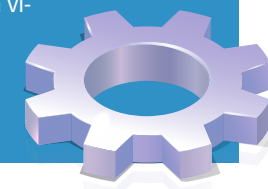
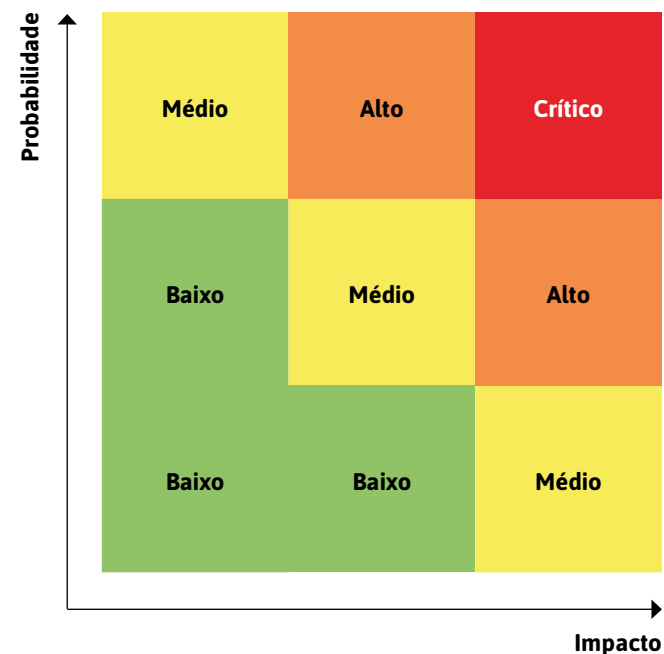




Gráfico 6. Matriz de risco



Análise dos riscos

A finalidade desta etapa é determinar quais incidentes podem ocorrer com base nas informações com as quais a organização conta. Existem diversos métodos para avaliar o nível de risco associado a cada incidente em potencial. Um dos métodos mais comuns é usar uma fórmula:

$$\text{Risco} = \text{Impacto} \times \text{Probabilidade}$$

A fórmula baseia-se no padrão ISO 31000, que define o risco como um produto da intensida-

de dos danos em potencial com a probabilidade de sua concretização (quais serão os danos sofridos se o incidente ocorrer, e qual é a probabilidade de que ocorra?).

Cálculo da magnitude dos danos

Realizado geralmente durante a análise dos danos em potencial máximos decorrentes de uma violação da confidencialidade/integridade/disponibilidade (CID) dos dados. Para calcular a magnitude, recomenda-se utilizar a Tabela 4.

Tabela 4. Questionário para determinar o cálculo da intensidade dos danos

Pergunta	Nível 1	Nível 2	Nível 3	Nível 4
<p>1. Qual é o nível de danos que a organização sofrerá após a divulgação das informações do processo/propriedade?</p> <p>C Confidencialidade</p>	<p>Os danos estimados satisfazem um ou mais dos critérios a seguir:</p> <p>A) custo de até US\$ 1,5 milhão para a organização;</p> <p>B) investimento de até dois meses de trabalho humano para sanar o incidente;</p> <p>C) a propriedade é definida como um banco de dados gerenciado por um indivíduo nos termos dos Regulamentos de Proteção da Privacidade (Segurança da Informação).</p>	<p>Os danos estimados satisfazem um ou mais dos critérios a seguir:</p> <p>A) custo entre US\$ 1,5 e 3 milhões para a organização;</p> <p>B) um investimento de mais de seis meses de trabalho humano, mas menos de cinco anos, para sanar o incidente;</p> <p>C) a propriedade é definida como um banco de dados com um nível baixo de segurança, segundo os Regulamentos de Proteção da Privacidade (Segurança da Informação).</p>	<p>Os danos estimados satisfazem um ou mais dos critérios a seguir:</p> <p>A) custo de mais de US\$ 3 milhões para a organização;</p> <p>B) investimento de mais de cinco anos de trabalho humano para sanar o incidente;</p> <p>C) “ativo” é definido como um banco de dados com um nível médio de segurança, conforme os Regulamentos de Proteção da Privacidade (Segurança da Informação);</p> <p>D) há um perigo em potencial de morte.</p>	<p>Danos significativos serão causados que cumprem pelo menos um dos seguintes critérios:</p> <p>A) há um perigo óbvio e imediato de morte de várias pessoas;</p> <p>B) danos econômicos estimados em mais de US\$ 30 milhões;</p> <p>C) a propriedade é definida como um banco de dados com um nível alto de segurança, segundo os Regulamentos de Proteção da Privacidade (Segurança da Informação);</p> <p>D) há um perigo óbvio para a saúde pública;</p> <p>E) existe um risco de morte óbvio.</p>
<p>2. Qual é o nível de danos que a organização sofrerá como resultado da invasão de informações (ou dados) do processo/propriedade?</p> <p>I Integridade</p>				
<p>3. Qual é o nível de danos que a organização sofrerá após a desativação/encerramento do processo/propriedade por um período prolongado?</p> <p>D Disponibilidade</p>				



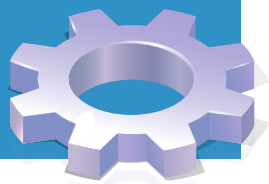
A pontuação de cada processo/ativo é a pontuação mais alta obtida para as três perguntas (Impacto = máx. 1-4). Essa pontuação também é chamada de **magnitude** do risco (marcada com a letra I). Ela define o potencial máximo de danos à organização em decorrência dos danos a este processo/ativo.

Atenção. Nos ramos de Defesa Cibernética e Segurança da Informação, é comum dividir os danos que podem ser causados nas três categorias abaixo.

Violação da confidencialidade dos dados: por exemplo, um ciberataque que vaze informações de clientes ou um segredo comercial na internet.

Comprometimento da confiabilidade dos dados: por exemplo, um ciberataque que altera os dados dos relatórios financeiros da empresa, de modo que não representem fielmente sua situação, ou um ataque que atrapalhe o funcionamento correto da linha de produção.

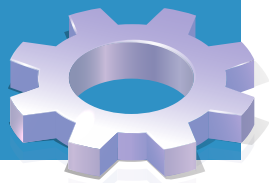
Violação da disponibilidade dos dados: por exemplo, um ciberataque que torna as informações indisponíveis para a empresa ou seus clientes. Por exemplo, quando um site fica fora do ar ou arquivos são bloqueados (*ransomware*).



Dica: vieses são comuns na avaliação dos valores de propriedades

A análise do valor dos ativos deve ser realizada em colaboração com os departamentos da empresa. No lado comercial, os proprietários podem sentir-se “supervalorizados”, acreditando que sua propriedade é a mais importante na organização. Cumprir os critérios do questionário de valores neutralizará esses sentimentos e ajudará a avaliar os sistemas em uma escala uniforme e não enviesada.

Observe que o comprometimento da confiabilidade dos dados pode ter implicações para os processos nas instalações físicas. Portanto, durante o processo de avaliação de riscos, é importante analisar o significado do ciberataque contra sistemas operacionais, controladores industriais (ICS), câmeras de segurança, sistemas de controle e monitoramento, ou equipamentos que muitas vezes não são gerenciados por equipes de TI.



O cálculo do grau de probabilidade pode ser baseado em uma ponderação de vários parâmetros.

A seguir, exemplos de parâmetros que podem ser levados em consideração.

01

Histórico de incidentes: uma visão geral dos ciberincidentes que ocorreram nos últimos anos, analisando o setor de atuação da empresa, suas características, seus sistemas típicos, etc. O objetivo é entender os tipos de ataque conhecidos no mundo e a frequência e predominância de cada um deles. Entender as tendências no mundo dos ciberataques ajuda a definir o peso dos incidentes recentes, em preparação para os desafios atuais enfrentados pela organização/setor.

02

Ciberinteligência: pesquisar informações na internet (por meio de recursos internos ou da aquisição de um serviço externo) permitirá que a organização obtenha um quadro geral mais preciso e se prepare para uma defesa de ponto a ponto baseada na imagem vista da perspectiva do agressor.

03

Facilidade de concretização: a facilidade de concretização do ataque pode ser afetada por diversas variáveis, como o tamanho da superfície de ataque (incluindo a quantidade de usuários e o tipo), o nível de defesa e a facilidade de acessar o ativo fisicamente, a quantidade de interfaces e o tipo, ou possíveis planos de ação do oponente em relação aos caminhos cruciais (caminhos de entrada e saída da organização).

04

Motivação do ataque e tipo de informação: o tamanho do banco de dados, o tipo de banco de dados, a identidade de seu proprietário, a existência de concorrentes comerciais e outras partes muitas vezes afetam a motivação de várias partes interessadas para atacar a organização. Por exemplo, sistemas que incluem informações médicas e/ou financeiras estão expostos a um nível diferente de ameaça que sistemas com informações de tipos diferentes.

Ponderar a motivação, os tipos de informação, as partes interessadas e os danos em potencial pode ajudar a organização a traçar um mapa de riscos mais preciso, levando em consideração a visão do oponente.

A Tabela 5 pode ser usada como ferramenta para apoiar a tomada de decisão durante o processo.

Tabela 5. Orientação sobre como analisar a perspectiva do oponente

 <p>Atores</p>	 <p>Motivação</p>	 <p>Meta</p>	 <p>Efeito/influência</p>
<ul style="list-style-type: none"> • Governo/emissários/patrocínio • Organizações criminosas • Funcionários com privilégios • Organizações terroristas • Ativistas • Concorrente comercial • Um <i>hacker</i> habilidoso que atua sozinho • <i>Script Kiddies</i> 	<ul style="list-style-type: none"> • Espionagem • Forças Armadas • Informações pré-missão • Política • Lucro financeiro • Desabilitação/interrupção/sabotagem • Vantagem competitiva • Anarquia/caos • Vingança/rancor • Tática/estratégia • Social/moral • Emissão de uma declaração 	<ul style="list-style-type: none"> • Danos e alteração das informações • Propriedade intelectual • Serviços • Filtro de informações sensíveis • Imagem e reputação 	<ul style="list-style-type: none"> • Ameaça à vida/segurança • Perda de renda/danos econômicos • Furto de IP • Danos à reputação • Destruição da infraestrutura • Denúncia/processo • Sanções e restrições • Perda da confiança do público/investidores • Interrupção da continuidade das operações • O ambiente • Percepção

A Tabela 6 pode ser usada para calcular a probabilidade. Uma pontuação de 1 a 4 deve ser atribuída a cada parâmetro/tese. Nos parâmetros compostos por várias subseções, cada seção recebe sua própria pontuação (entre 1 e 4); em seguida, calcula-se a média das pontuações de todas as seções.

Tabela 6. Ferramenta para calcular a probabilidade de acordo com os parâmetros

Parâmetro/critério	Perguntas auxiliares
Histórico de incidentes (valor que vai de 1 a 4)	Ocorreu algum ciberincidente na organização e/ou nas instalações dos fornecedores da organização nos últimos cinco anos?
Informações sobre ciberameaças (valor que vai de 1 a 4)	Os achados de ciberinteligência indicam que as informações detidas pela organização são um alvo de ataque preferencial? Os achados de ciberinteligência indicam que a organização e/ou os fornecedores da organização e/ou organizações em setores semelhantes de Israel ou do mundo todo constituem um alvo de ataque preferencial?
Qual é a superfície de ataque? (valor que vai de 1 a 4)	Qual é o nível de segurança física do processo/propriedade? Quais são a política de atualização e os patches de segurança? Qual é o nível de atualização do processo/propriedade? Qual é o nível de compartimentalização de privilégios no sistema? O sistema pode ser acessado remotamente? Que tipos de informação estão presentes no sistema? Qual é a natureza das interfaces do processo/propriedade? Quantas interfaces o sistema tem? Quem são os usuários humanos do processo/propriedade? Qual é a quantidade de usuários (humanos/aplicativos/computadores) do processo/propriedade?

Agora, a pontuação atribuída a cada parâmetro deve ser inserida na fórmula abaixo. Atenção: é possível atribuir um coeficiente a cada parâmetro com uma magnitude diferente, dependendo de sua importância para a organização (o valor total dos coeficientes deve ser 1). No exemplo apresentado aqui, o parâmetro de superfície de ataque recebeu a maior importância (coeficiente de 0,5), enquanto o parâmetro de histórico de incidentes foi considerado menos importante (com um coeficiente de apenas 0,2).

$$\{0,5 \times (\text{pontuação da superfície de ataque}) + 0,3 \times (\text{pontuação das informações}) + 0,2 \times (\text{pontuação do histórico de incidentes})\} = \text{Probabilidade}$$

Cálculo do nível de risco ao ativo: como os dados são ponderados

01

Risco inerente: calculado com base na ponderação da intensidade do potencial de danos (impacto), derivada do valor do alvo de defesa, e no grau de probabilidade de ocorrência de um ciberincidente na propriedade ou processo em questão (probabilidade).

Para efetuar o cálculo, colocamos os valores da intensidade/valência (I) e da probabilidade (P) na matriz apresentada na Tabela 7 (o risco aumenta conforme o número e a cor passam de verdes para vermelhos).

02

Risco residual: como as organizações implementam controles de defesa, como gestão de acessos, criptografia ou permissões de monitoramento, o nível de risco que enfrentam de fato é inferior ao nível de risco original. Após ponderar os controles existentes na prática, o nível de risco é representado pelo valor chamado de “risco residual”.

Às vezes, para reduzir o risco, a organização pode reduzir o potencial de sofrer danos (impacto); por exemplo, criando um sistema de back-up eficaz ou adquirindo um seguro cibernético. No entanto, na maioria das vezes, para reduzir o risco, a organização reduz a área de exposição e a probabilidade de concretização de um ciberincidente. Isso é feito por meio da adoção de controles, tecnologias, procedimentos e processos de defesa.

Tabela 7. Cálculo do nível de risco de um ativo

		Probabilidade (P)				
		1	2	3	4	Impacto (I)
Impacto (I)	4	7	10	13	16	4
	3	6	9	12	15	3
	2	5	8	11	14	2
	1	4	7	10	13	1

Para calcular o risco residual, o nível de risco (calculado na matriz acima) precisa ser reduzido de acordo com o nível real de implementação dos controles existentes. Assim, o nível de risco residual pode ser representado pela seguinte fórmula:

(Impacto (I) x Probabilidade (P)) – Controles

Eis aqui dois exemplos de como avaliar em quantos níveis a implementação dos controles reduzirá o risco:

- um teste que mostrará, por exemplo, que a implementação de todos os controles reduzirá o nível de risco em dois níveis, enquanto a implementação de 50% deles causará uma redução em um nível;
- realização de uma avaliação de riscos (intensidade e razoabilidade), supondo-se que a organização implemente os controles que decidiu incorporar ao plano de redução.

2.2 Análise de riscos

Após formular uma lista de riscos e/ou ameaças classificados de acordo com a prioridade de tratamento, cada um deles precisa ser avaliado em contraste com o nível de risco que a organização pode aceitar.

Risco do alvo. Quando o nível de risco residual é superior ao nível de risco aceito pela organização (conhecido como apetite de risco), um plano de mitigação precisa ser elaborado com o objetivo de reduzir o risco residual até o nível de risco desejado (a menos que a administração tenha decidido seguir uma estratégia de gestão de riscos diferente, como por meio de transmissão ou aceitação dos riscos).

Uma análise da literatura profissional revelou que não existe um método e/ou uma fórmula internacional aceita para calcular o risco do alvo. Portanto, uma das duas alternativas a seguir pode ser usada.

01

Utilização do método de gestão de risco da sua organização (riscos de conformidade, riscos de crédito, riscos operacionais, etc.).

02

Utilização das diretrizes a serem definidas pela organização, como a estipulação de um risco máximo que a mesma organização é capaz de conter (por exemplo, uma decisão de não atingir um nível de risco acima de 10), elaboração de um plano para mitigar os riscos encontrados no mapa de calor acima desse valor e redução dos riscos altos.

Para definir o risco do alvo e o apetite de risco em função do risco original, uma ferramenta como a Tabela 8 pode ser usada.



Tabela 8. Ferramenta para definir o risco objetivo e o comportamento de risco

	Potencial de danos			
	1	2	3	4
Prejuízos humanos	Nenhum risco evidente	Leve risco para a saúde das pessoas ao redor	Grave risco para a saúde dos funcionários ou clientes	Risco de perda de vidas
Prejuízos econômicos	Custo de até US\$ 1,5 milhão para a organização	Custo de US\$ 1,5 a 3 milhões para a organização	Custo de mais de US\$ 3 milhões para a organização	Prejuízo econômico estimado em mais de US\$ 30 milhões
Prejuízos funcionais	Investimento de até dois meses de mão de obra para gerenciar o incidente até o retorno à normalidade. Pequenos prejuízos ao serviço prestado aos clientes e às partes interessadas	Investimento de mais de seis meses e menos de cinco anos em mão de obra para gerenciar o incidente até o retorno à normalidade. Prejuízos médios ao serviço prestado a clientes e partes interessadas	Investimento de mais de 5 anos em mão de obra para lidar com o incidente. A organização sofrerá prejuízos irrecuperáveis ou prejuízos graves e contínuos à continuidade operacional	Perigo de fechamento da organização em decorrência do incidente
Prejuízos à imagem	Não são esperados prejuízos consideráveis à imagem	A organização sofrerá prejuízos à sua imagem durante o gerenciamento do incidente. Possibilidade de ações judiciais coletivas	A organização perderá uma vantagem competitiva e também seu posicionamento em relação aos concorrentes e clientes	A organização perderá a confiança dos clientes e enfrentará severas críticas do público
Prejuízos sociais, ambientais ou públicos	Pequenos prejuízos à continuidade do serviço aos clientes da empresa	Prejuízos médios aos clientes ou fornecedores da organização (cadeia de suprimentos)	Prejuízos graves à privacidade dos funcionários ou clientes da organização	Prejuízos graves e irreversíveis ao meio ambiente
Prejuízos à confidencialidade das informações	No caso de um ataque de <i>ransomware</i> envolvendo roubo de dados, os prejuízos econômicos são estimados entre US\$ 500.000 e US\$ 1 milhão	Temor de prejuízo financeiro devido à perda de informações gerada por um <i>insider</i> , com ênfase naqueles com privilégios elevados no sistema internacional de gerenciamento de relacionamento com o cliente (CRM)	Vazamento de todo o banco de dados médicos, causando prejuízos irreversíveis aos clientes da organização	
Prejuízos à disponibilidade de informações e à continuidade operacional	No caso de um ataque de <i>ransomware</i> , estima-se que será necessária uma semana para a recuperação e o upload dos backups. Haverá pequenos prejuízos à continuidade dos negócios		No caso de prejuízos à linha de produção (ICS) devido a um incidente cibernético, são esperados prejuízos de dezenas de milhões de dólares, com prejuízos significativos à continuidade operacional	
Prejuízos à confiabilidade das informações e dos dados	Prejuízos financeiros que chegam a centenas de milhares de dólares como resultado do trabalho com informações armazenadas em aplicativos que não permitem trilha de auditoria, gestão de privilégios, gestão de versões, etc. Se as informações forem alteradas, serão necessários vários meses de trabalho para corrigir e restaurar os dados	No caso de violação do processo de relatórios para a bolsa de valores e de alteração dos dados do demonstrativo financeiro, os prejuízos à organização incluirão prejuízos à sua imagem e custo financeiro estimado em vários milhões de dólares		Cancelamento de ordens de serviço e contratos com a organização, até e incluindo o risco de fechamento, devido à alteração de dados no principal banco de dados da organização que contém informações de importância vital para o serviço prestado aos clientes

2.3 Avaliação de riscos

Neste estágio, realiza-se uma avaliação dos riscos analisados e toma-se uma decisão de como lidar com esses riscos.

A decisão precisa levar em conta as seguintes considerações, entre outras: quão crucial o processo comercial é; a topologia da organização; os sistemas de informação e prestadores de serviços ou produtos que estão envolvidos nos processos cruciais; e a capacidade de responder e tratar os riscos.

Neste estágio, a organização contará com uma tabela de resumo dos riscos identificados e classificados. A Tabela 9 é um exemplo.

No fim deste estágio, a organização contará com um mapa de ameaças/ riscos classificados.

Tabela 9. Resumo dos riscos identificados e classificados

Nome do risco	Descrição do caso	Probabilidade (de 1 a 4)	Intensidade (de 1 a 4)	Risco original (poder e probabilidade)	Qualidade dos controles existentes	Risco residual
Perda de vantagem competitiva em decorrência do vazamento de informações sensíveis	Posse não autorizada de informações por parte de um funcionário da organização por meio de um dispositivo de memória portátil ou envio por e-mail particular/profissional					
Perda de receita em decorrência da desabilitação da comunicação entre filiais	Um incidente de <i>ransomware</i> na rede corporativa/ organizacional					
Exposição judicial decorrente de uma não conformidade com a legislação e/ou a regulamentação	Divulgação não controlada de informações por um provedor por meio de um serviço de nuvem					
Perda de renda decorrente da incapacidade de liberar transações	Ataque de negação de serviço contra o site da empresa					
Danos à reputação decorrentes de uma intrusão nos sistemas de um dos principais fornecedores da organização	Utilização de uma interface de acesso remoto à organização por meio de um fornecedor da organização					

Estágio 3: tratamento dos riscos

Como regra geral, é impossível realizar uma atividade sem nenhuma exposição a riscos.

Os esforços de mitigação dos riscos devem ser acompanhados pela ponderação de diversos parâmetros: teste de custo-benefício econômico para a organização; duração da implementação; nível de probabilidade de concretização do risco; obrigações legais da organização em virtude dos contratos assinados com fornecedores e/ou por força da lei e dos regulamentos; considerações morais (por exemplo, responsabilidade social); e outros parâmetros acordados pela administração da organização.

No fim deste estágio, a organização categorizará cada risco de acordo com as quatro opções comumente usadas para lidar com riscos no mundo todo, como segue.

01

Aceitação do risco: se o risco não for alto, a organização pode decidir realizar a atividade de sem implementar controles de defesa exclusivos. É possível que a organização decida aceitar o risco mesmo quando as medidas necessárias para reduzi-lo ultrapassem o limite de recursos que a organização está disposta a investir em resposta à ameaça em questão. Por exemplo: a organização pode decidir que seus computadores serão acessados sem um processo de identificação robusto devido ao

custo associado à implementação de um mecanismo de identificação robusto ou à atribuição de um peso baixo ao risco de vazamento de informações do sistema.

02

Redução do risco: se a atividade da organização precisar ser realizada apesar dos riscos inerentes a ela, é possível avaliar a implementação de controles de defesa que reduzam a probabilidade de concretização de um ciberincidente. Por exemplo: se a organização possuir estações de vendas que liberem transações com cartões de crédito, é comum aplicar controles de defesa para reduzir o risco de vazamento dessas informações de crédito. Esses controles podem incluir evitar que dispositivos externos se conectem, gerenciar os privilégios das estações de trabalho, criptografar os dados sensíveis, entre outros.

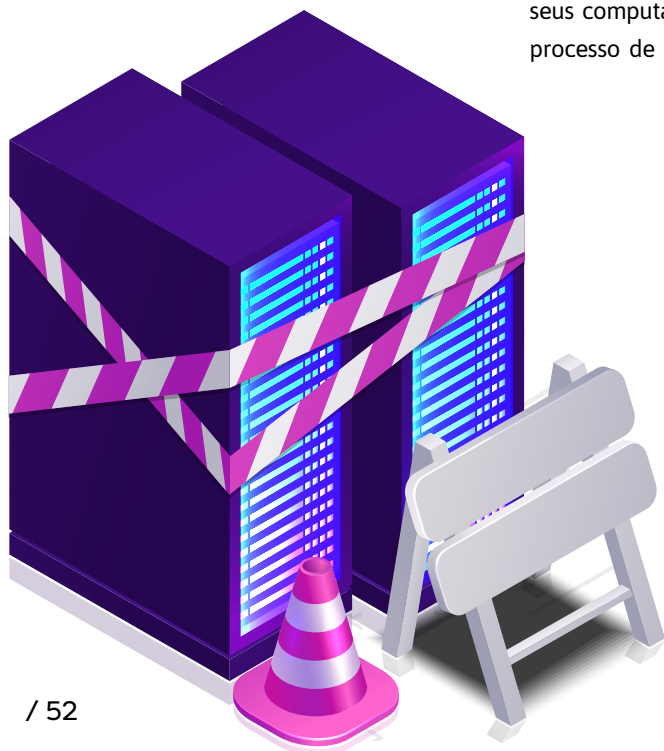
03

Transferência do risco: caso a atividade precise ser realizada, mas a organização não esteja interessada em dispor dos recursos de defesa necessários (conhecimento, ferramentas, força de trabalho, etc.), a atividade pode ser transferida para um terceiro. Por exemplo: se a organização estiver interessada em criar um site ou perfil nas redes

sociais, mas não contar com os recursos necessários para protegê-los, a execução pode ser transferida para um subcontratado, que configurará e protegerá o site/perfil. Outra opção de transferência do risco é adquirir um seguro cibernético que cubra o risco em questão. Porém, deve-se levar em consideração que, muitas vezes, a lei não isenta a organização da responsabilidade no caso de um ciberincidente como, por exemplo, vazamento de informações pessoais.

04

Evitar o risco: quando o nível de risco é muito alto, bem como a probabilidade de concretização desse risco, a organização pode optar por adiar o risco, “redefinindo a probabilidade de sua concretização”. Por exemplo: se a administração da organização entender que não possui o conhecimento e as ferramentas necessários para proteger o banco de dados que pretende estabelecer, pode decidir não manter esse banco de dados ou não armazenar informações muito sensíveis nele.



Aplicação dos controles de defesa

Assim que a organização decidir os ativos/processos por meio dos quais a atividade de redução do risco será realizada, será necessário criar os controles de defesa correspondentes. Os controles consistem em processos, produtos e pessoas que realizam várias atividades para reduzir os riscos cibernéticos à organização, como: gestão de usuários, criptografia, monitoramento e back-ups, entre outros. O nível de

defesa de cada ativo/processo é afetado diretamente pelo seu nível de risco residual.


A rotina de defesa cibernética consiste na elaboração, implementação e assimilação de controles de defesa. Este capítulo forma as bases dessa rotina e, em prol de sua implementação, deve-se utilizar o Apêndice C deste documento e o banco de dados de controles da Metodologia de Defesa Cibernética disponibilizado no site da Diretoria Cibernética Nacional de Israel.²

É comum apresentar os vários controles dentro da estrutura de conceitualização que reflete as conexões entre eles (Estrutura). Controles exclusivos foram criados pela Diretoria Cibernética Nacional de Israel conforme as definições de ameaças mais recentes e incorporados a uma estrutura semelhante à Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST). Esses controles possibilitam a utilização do conhecimento e da experiência profissionais vastos do departamento local de

segurança cibernética e, ao mesmo tempo, permitem que as organizações atuem de acordo com as estruturas de trabalho aceitas internacionalmente.

Os controles da Metodologia de Defesa Cibernética têm características únicas, incluindo a construção da “profundidade de aplicação da implementação”, a inclusão de ênfases para otimizar a implementação de um controle específico, bem como o foco e os indícios necessários para construir uma infraestrutura profissional de certificação para este método.

Tabela 10. Estrutura de controles da Metodologia de Defesa Cibernética

Identificação	Proteção	Deteção	Resposta	Recuperação
<ul style="list-style-type: none"> Responsabilidade da administração e da diretoria Gestão de riscos e avaliação de riscos 	<ul style="list-style-type: none"> Controle de acessos Proteção das informações Computação em nuvem Defesa dos objetivos de proteção Proteção de estações de trabalho e servidores Proteção física e ambiental O fator humano Proteção de ambientes de TO Segurança de rede Criptografia 	<ul style="list-style-type: none"> Metodologia e procedimentos profissionais de proteção das informações de monitoramento cibernético Defesa cibernética proativa (mapeamento) Coleta e proteção de artefatos Sistema de monitoramento central Análise 	<ul style="list-style-type: none"> Gestão e geração de relatórios de incidentes 	<ul style="list-style-type: none"> Continuidade dos negócios 

2. Consulte a ferramenta ICDM Controls, disponível em:

https://www.gov.il/en/departments/general/cyber_security_methodology_2

Para decidir quais controles são relevantes para um ativo/processo comercial cujo nível de risco precisa ser reduzido, confira a lista de controles de defesa no Apêndice 3. Realize o processo de “análise de lacunas”, definindo a profundidade de aplicação necessária para cada controle adotado.

No fim deste processo, a organização receberá uma lista de lacunas e controles necessários, dependendo da profundidade de aplicação de cada controle.

Como cada controle está associado a riscos e processos diferentes, às vezes, as organizações optam por implementar a análise dos controles “de forma contínua”, utilizando-os como uma lista de verificação.

A principal desvantagem desse método é o fato de que a organização avalia os controles

conforme sua conformidade com regulamentos/normas, não a partir de uma perspectiva baseada no risco (baseada no risco versus baseada no controle).

Como nem todos os controles são implementados da mesma forma na organização e nem todos os controles são necessários para cada processo/ativo, certifique-se de realizar um teste separado para cada alvo de defesa relevante para a organização. A experiência mostra que, embora os controles geralmente sejam implementados em organizações de todos os tipos, existem casos raros em que o controle não é implementado em um processo/sistema específico.

Como nem todos os controles são necessários para cada ativo, use o nível de valor definido para cada ativo no Estágio 3 para traçar a lista de lacunas. Essa lista servirá de base para formular o plano de trabalho da organização (Estágio 4).

No fim deste estágio, a organização contará com uma lista como a da Tabela 11.

Tabela 11. Lista de controles

Controle	A organização toda	O sistema de CRM	Sistema de Pagamento de Fornecedores
A autenticação multifatorial precisa ser implementada para fazer login em contas com privilégios na rede, dependendo da profundidade de aplicação	Parcialmente presente	Presente	Precisa ser concretizado/materializado
Medidas de segurança precisam ser definidas e implementadas para detectar e alertar sobre alterações não autorizadas nas configurações, dependendo da profundidade de aplicação	A organização conta com um processo ordenado	O sistema está na nuvem, e não temos controle direto sobre a implementação deste requisito, mas os requisitos podem ser exigidos do fornecedor	Presente
Ferramentas contratuais e judiciais devem ser usadas ao adquirir um sistema de informação ou prestador de serviços, dependendo da profundidade de implementação	Não existe um processo ordenado de obtenção de assinaturas dos fornecedores na organização	O fornecedor assinou uma declaração	Trata-se de um fornecedor estrangeiro cuja assinatura não pode ser obtida. Vamos analisar os requisitos conforme o acordo genérico com o fornecedor

Estágio 4: formulação de um plano de trabalho

Depois de mapear os objetivos de defesa e examinar os controles que devem ser implementados na organização para reduzir o risco residual (de acordo com a profundidade de cada aplicação selecionada), deve-se realizar um processo de priorização e definir um plano de trabalho para implementá-lo.

A fim de otimizar a ordem de ações e maximizar os benefícios derivados dos recursos alocados no plano de trabalho, vale a pena considerar a visão do oponente. É importante notar que boa parte das informações necessárias para completar este estágio devem advir do Estágio 2 - “cálculo do grau de probabilidade”.

A classificação de agressores e ataques pode ser organizada de acordo com a divisão a seguir.

01

Fonte de ataque: equipe interna da organização, parceiro externo/ terceiros à organização, uma equipe/parte que é externa à organização.

02

Motivo do ataque/incidente: acidental ou intencionalmente.

Esta divisão apresentará à organização uma matriz para ajudar a organização a se concentrar em ameaças que precisam de mais atenção, por exemplo: um funcionário mal-intencionado que tenta extrair informações confidenciais da organização; um provedor de serviços terceirizado que inadvertidamente causa dano como resultado de seu baixo nível de defesa; ou um ataque externo dirigido a prejudicar a organização ou obter benefícios.

Esta abordagem pode priorizar a organização e ajudá-la a classificar áreas de risco nas quais não foram investidos recursos para resolvê-los.



Porém, uma análise de muitos incidentes mostrou que, na grande maioria dos ciberataques, um dos canais a seguir foi usado.

01

Abuso de interfaces externas tais como RDP, SSH ou FTP.

02

Introdução de *malware* pelo envio de um e-mail com um arquivo malicioso ou um link para um site malicioso.

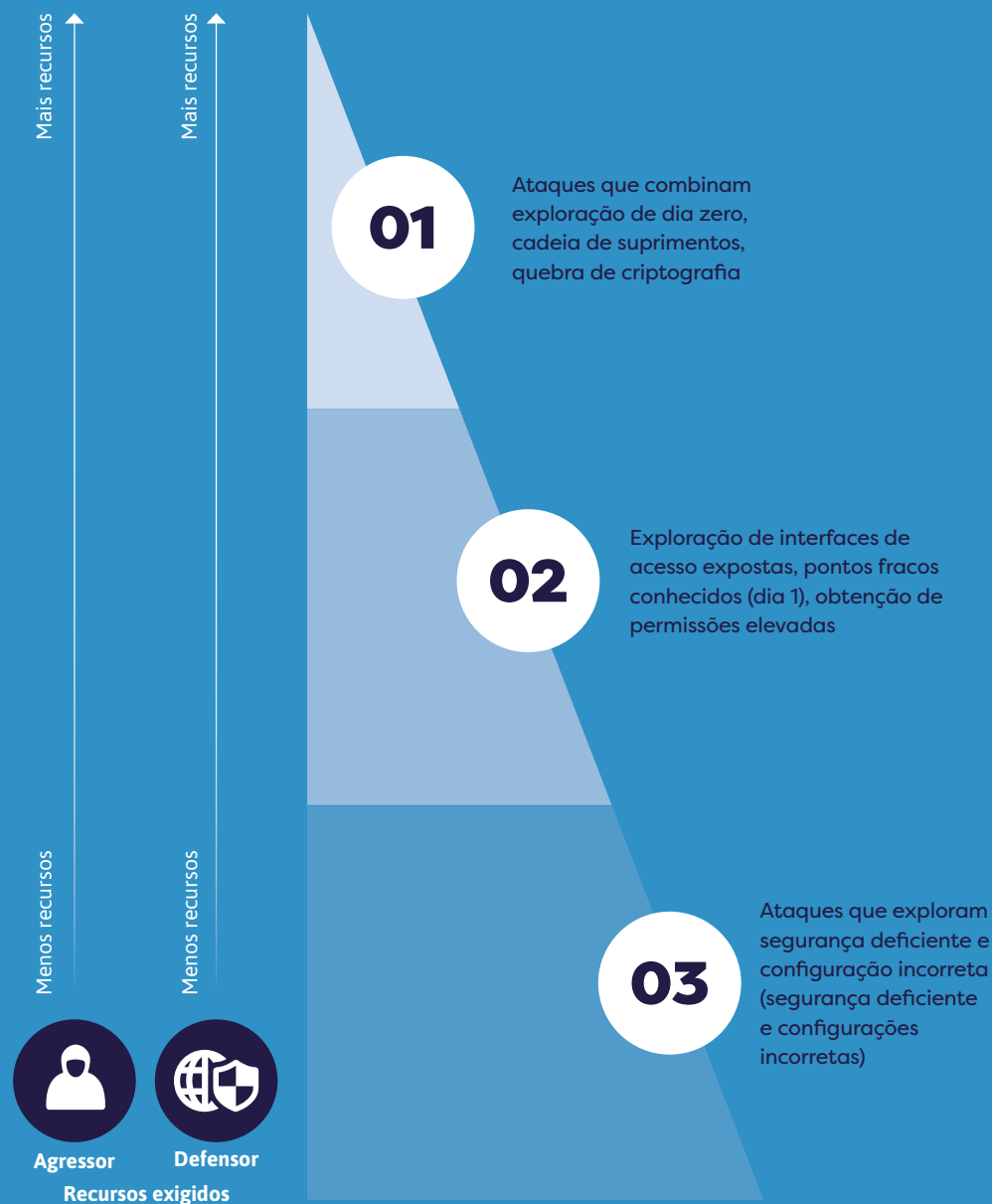
03

Navegação em sites infectados que baixam *malware* na estação de trabalho.

Um ataque que não é realizado diretamente pela internet exige do agressor muitos recursos e a ativação de meios adicionais, como o uso de engenharia social, a utilização da cadeia de suprimentos, a realização de operações de enterro ou a obtenção de acessibilidade física. Todos eles tornam o ataque mais complexo e mais caro.

Essa perspectiva orienta a organização a dar maior prioridade a projetos que dificultem que o agressor acesse a rede da organização e se aposses dela. Tais projetos incluem, entre outros, a proteção de interfaces (ou seja, implementação de autenticação multifatorial), a proteção do servidor de e-mails da empresa (ou seja, uso de retransmissão de e-mails, *sandbox*), e o fortalecimento de interfaces para minimizar o uso de protocolos perigosos.

A implementação de processos de fortalecimento e medidas de defesa para esses caminhos pode fornecer uma solução às duas camadas mais baixas da pirâmide a seguir.

Gráfico 7. Ataques e aproveitamento de vulnerabilidades

Deve-se considerar que organizações diferentes estão sujeitas a riscos cibernéticos diferentes, que têm origem na natureza e características exclusivas da organização. Assim, por exemplo, uma organização cuja fonte principal de renda seja seu site de comércio pode preferir investir em medidas de defesa do site (como Anti-DDoS ou WAF) em vez de proteger as caixas de e-mail corporativas.

Entretanto, para a maioria das organizações no mundo, a defesa dos canais de penetração da internet nas diversas interfaces é a base mínima exigida para lidar com a maior parte dos tipos de ataques.

A melhoria contínua do nível de resiliência de uma organização diante da ameaça de atribuição que ela enfrenta pode se refletir na adoção e assimilação de controles de níveis mais altos (como controles dos níveis 3 e 4). A melhoria também se refletirá no aprofundamento da eficácia dos controles (“profundidade de implementação do controle”).

Formulação e adoção de uma percepção avançada para lidar com ameaças avançadas

Uma organização que precisa enfrentar ameaças mais avançadas, mais frequentemente atribuídas a grupos de ataque avançados ou atacantes estado-nação, deve fazer seu planejamento baseado em uma **percepção de defesa** mais complexa.

A percepção de defesa avançada inclui considerar: a capacidade da organização de produzir dissuasão no ciberespaço, a política da organização em relação à caça de ameaças, inteligência proativa, programas de recompensa de bugs, e a variabilidade da topologia de defesa e dos processos executados na organização. A abordagem exige amadurecimento organizacional e diálogo com a administração sobre a “percepção da organização” para lidar progressivamente com as ciberameaças. Por exemplo, o uso de mecanismos alternativos e redundâncias de infraestrutura tecnológica pode permitir que uma organização cujo site deixou de funcionar continue prestando serviços/fornecendo informações sem interromper suas atividades de negócios.

Exemplos de componentes no desenvolvimento de um conceito de defesa organizacional são apresentados no Apêndice 7 deste documento.

Estágio 5: auditoria e monitoramento contínuos

A gestão de riscos é um processo que consiste em uma série de estágios de trabalho definidos, que a organização executa ciclicamente ao longo dos anos. O propósito da tabela periódica é atualizar periodicamente o mapa de riscos e as respostas necessárias. Essa atualização é importante, entre outras razões, devido tanto à implementação de controles de defesa como às mudanças nos espaços interno e externo da organização.

Além disso, as organizações vêm trabalhando para elevar o nível de resiliência cibernética ao longo dos anos por meio da adoção de processos de “melhoria contínua”.

Como tanto a realização de uma pesquisa de riscos abrangente em uma organização como a implementação das etapas requeridas após essa pesquisa levam muito tempo, em muitas organizações o processo é mais ou menos assim:

Gráfico 8. Ciclo de melhoria contínua



O processo de avaliação de riscos de uma organização leva alguns meses. Quando finalizado, um mapa dos riscos e das medidas necessárias para mitigá-los (o plano de trabalho) é apresentado à administração. Essas medidas formam a base para o planejamento do orçamento e do plano de trabalho plurianual da defesa cibernética dentro da organização. Esse plano pode incluir, entre outros, a necessidade de dar início a processos de aquisição, assimilar tecnologias de defesa e incorporar procedimentos na organização.

Este processo não é exclusivo da gestão de riscos cibernéticos e também é aceito em muitas outras áreas onde a organização gerencia seus riscos (como riscos de conformidade ou operacionais).

Como o ritmo da mudança é um fator crucial no mundo digital, e particularmente nos campos de defesa e ataque cibernéticos, as organizações precisam desenvolver a capacidade de realizar auditorias e monitoramentos com flexibilidade e rapidez. Isto é assim para que, a qualquer momento, possam responder à pergunta sobre **qual é o nível de proteção da organização contra ciberameaças e quais são os passos imediatos que ela deve dar para minimizar esses riscos?**

Juntamente com o planejamento orçamentário, o recrutamento e a capacitação de funcionários, e os processos de longo prazo decorrentes de uma pesquisa de risco horizontal, é necessário que a organização desenvolva uma capacidade independente de realizar auditorias e monitoramentos contínuos. Essa capacidade é chamada “Monitoramento de Controle Contínuo”, doravante CCM (na sigla em inglês).

Para desenvolver a capacidade de CCM e sua implementação eficaz, a organização deve formular um conceito que incluirá, entre outras coisas, os aspectos a seguir.

01

Análise da proteção da organização contra ataques que se originam na cadeia de suprimentos (Gestão de riscos da cadeia de suprimentos).

02

Análise da proteção da organização contra ataques que têm origem em ativos digitais sobre os quais não há nenhum controle operacional ou tecnológico (Defesa de riscos digitais e XaaS).

03

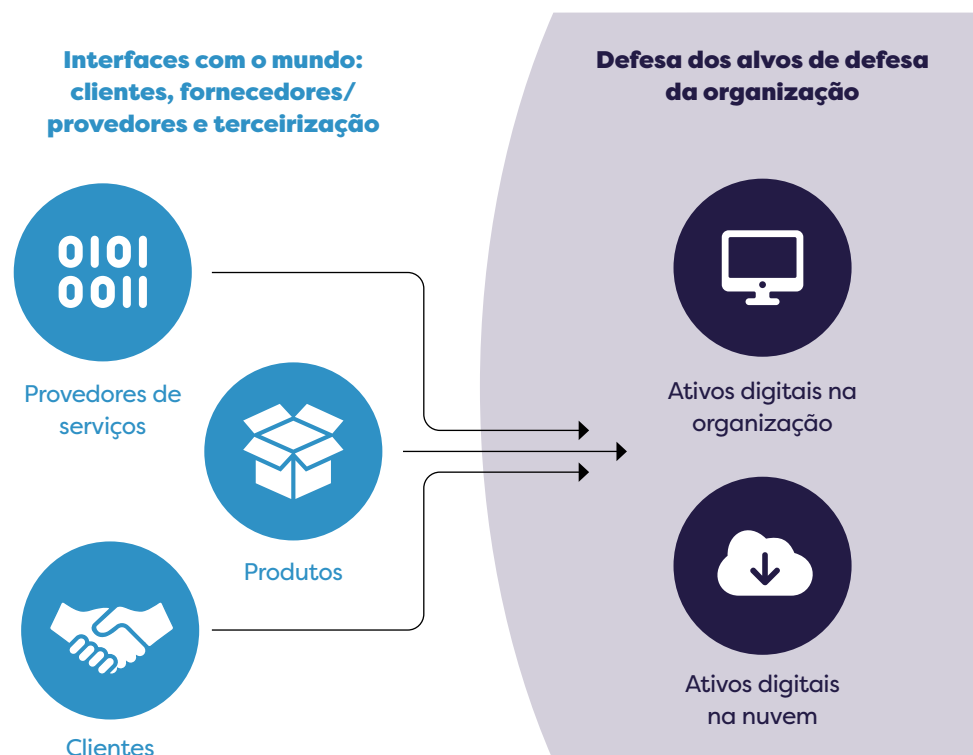
Análise da proteção da organização contra ataques que se originam em sua superfície de exposição, como ela aparece em termos de intenções e potenciais aos olhos do oponente. Isto se reflete principalmente na gestão da superfície de ataque, na varredura de

sua vulnerabilidade e no Simulador de Ataques e Violações.

04

Monitoramento permanente (24/7) da infraestrutura e dos sistemas, seja de forma independente, seja por meio de serviços terceirizados.

Gráfico 9. Uma visão holística dos riscos cibernéticos na organização



No passado, a maioria dos esforços de defesa baseava-se na visão da organização como uma unidade orgânica fechada e demarcada. A aceleração do uso da nuvem, junto com a dependência cada vez maior de provedores de serviços e produtos, tornou difusos os limites da organização. Muitos ativos digitais que a organização usa, como redes sociais, serviços de armazenamento, sistemas como CRM e ERP e inclusive serviços de e-mail agora são fornecidos na configuração "software como serviço" (SaaS, na sigla em inglês). Esta realidade exige que a organização examine holisticamente seus riscos cibernéticos internos e externos, bem como sua capacidade de monitorar, responder e recuperar-se.

Estas informações costumam ser gerenciadas por diversas ferramentas e serviços na organização, incluindo:

01

Sistema de Gestão de Riscos Cibernéticos (Gestão de riscos de provedores, VRM na sigla em inglês).

02

Sistema de coleta de inteligência cibernética (CTI, na sigla em inglês) e gestão de defesa de ativos digitais (Defesa contra riscos digitais, DRP na sigla em inglês) como contas de usuários em redes sociais.

03

Um sistema para o mapeamento da superfície de exposição da organização (Gestão da superfície de ataque, ASM na sigla em inglês).

04

Sistema para examinar simulações de ataque (Simulador de ataques e violações, BAS na sigla em inglês).

A implementação eficaz deste plano criará uma imagem de espelho para a organização que refletirá seu nível de resiliência mesmo do ponto de vista do agressor. A imagem permitirá que a administração mostre o nível de amadurecimento e a prontidão da organização nos vários mundos de conteúdo, priorizando ameaças e vulnerabilidades.

Gráfico 10. Pós-ataque (compartilhamento de código e arquivo, desfiguração, dados confidenciais roubados, falsificação de marca)



Descrição do processo de ataque de acordo com o método *Cyber Kill Chain*

Enquanto o lado da defesa trabalha para reduzir a superfície de ataque em todos os canais e implementa controles de defesa como criptografia, identificação forte ou fortalecimento de estações, o lado do ataque pode ficar satisfeito com a localização de um caminho de intrusão bem-sucedido.

Devido à assimetria integrada entre o lado da defesa e o agressor, é necessário criar um mecanismo de priorização de tarefas. Refor-

çar permanentemente todas as estações de trabalho, atualizar todos os patches de segurança relevantes e conscientizar todos os funcionários e provedores são medidas que exigirão diversos recursos.

A utilização eficiente dos recursos da organização requer a capacidade de produzir em tempo real um instantâneo atualizado do mapa de oportunidades do oponente para executar o ataque. A imagem situacional deve ser graduada, com o objetivo de atingir o máximo valor permitido pelos recursos alocados à defesa. Esta classificação pode basear-se nos parâmetros a seguir.

01

No eixo humano: quem tem os mais altos privilégios dentro da organização? Quem são as partes que têm um perfil de alta exposição na mídia?

02

No eixo tecnológico: que sistemas são “extrovertidos” em relação à internet? Quais são as tecnologias que a organização usa e que qualquer ator na economia pode conhecer?

03

No eixo de processos: quais projetos recebem ampla cobertura da mídia? Quais são os processos que têm o maior impacto na consciência do público ou nas atividades de negócios da organização?

Analisar as informações sobre pessoas, processos e sistemas na organização que o oponente desejará obter para planejar ataques, pode ajudar a priorizar os esforços de defesa e criar dificuldades para o agressor no estágio da coleta (reconhecimento ativo e passivo).

Gráfico 11. Informações comuns que um agressor poderia estar procurando no estágio do Reconhecimento antes do ataque



Observação: DNS: serviço de tradução de endereços (sigla em inglês).

O Apêndice 4 inclui ferramentas e métodos recomendados para implementar o princípio de controle contínuo.

Apêndices

Apêndice 1. Controles de defesa de uma organização da categoria A – ênfase nos computadores

Tabela A1.1. Destaques para o profissional de TI

Família	Seção	O controle	Explicação complementar
Responsabilidade da administração	Governança corporativa	A abordagem da organização para gerenciar a segurança da informação e a defesa cibernética, e como ela é implementada, deve ser examinada periodicamente.	Os controles de segurança implementados na organização, as políticas de segurança da informação e a defesa de processos de negócios cruciais para a organização devem ser examinados.
Prevenção de código malicioso	Deteção e prevenção de código malicioso em estações de trabalho e servidores na organização	Devem ser implementadas as ferramentas apropriadas para detectar e prevenir códigos maliciosos em dispositivos finais e servidores na organização. Essas ferramentas serão ativadas em um formato de defesa ativo, sendo necessário executar varreduras periódicas.	Como alguns <i>malwares</i> podem se infiltrar através de mecanismos de segurança, é preciso assegurar que os controles de tratamento de códigos maliciosos também sejam implementados nas estações de trabalho.

Família	Seção	O controle	Explicação complementar
Prevenção de código malicioso	Atualizações automáticas	A atualização automática de todos os sistemas deve estar ativada para detectar e prevenir códigos maliciosos na organização.	A organização executará uma atualização automática em um servidor central gerenciado pela organização ou por um provedor de serviços reconhecido. Essas atualizações garantirão que as ferramentas de defesa sejam constantemente atualizadas.
Criptografia	Critérios de criptografia	Os usos que exigem criptografia e o tipo de criptografia requerido devem ser definidos segundo as leis, diretrizes, procedimentos, regulamentações e obrigações de negócios.	A organização determinará as informações e os sistemas a serem criptografados e documentará a configuração da criptografia das informações. Os requisitos serão derivados das exigências aplicáveis à organização ou dos requisitos para a manutenção da informação.
Proteção de estações de trabalho e servidores	Política de fortalecimento	Políticas de fortalecimento para estações de trabalho e servidores devem ser definidas, documentadas e implementadas. Elas fornecem uma solução aos requisitos de segurança das informações da organização.	A organização definirá os requisitos de fortalecimento para os sistemas na organização, enfatizando os requisitos básicos, a frequência de atualizações e o nível de classificação. Deverá, então, documentar os requisitos em uma superestrutura, que servirá como base para a redação dos procedimentos de fortalecimento.

Família	Seção	O controle	Explicação complementar
Proteção de estações de trabalho e servidores	Aplicação do fortalecimento	O sistema deve ser configurado para fornecer a funcionalidade mínima exigida, bloqueando funções, portas e protocolos desnecessários.	<p>A organização definirá procedimentos de fortalecimento para cada tipo de sistema e servidor a partir de práticas aceitas, de modo a incluir, no mínimo, as funcionalidades a seguir.</p> <ul style="list-style-type: none"> • Redução da área de ataque do sistema pelo bloqueio de portas desnecessárias. • Desativação de serviços desnecessários. • Remoção de contas de usuários convidados. • Preferência pelo uso de protocolos seguros na comunicação entre servidores. • Recepção de atualizações de forma ordenada. • Bloqueio de funções sensíveis do sistema. • Envio de logs de incidentes do sistema para o monitoramento do servidor. • Bloqueio da instalação de software por usuários não autorizados.

Família	Seção	O controle	Explicação complementar
Computação em nuvem pública	Responsabilidade compartilhada	A divisão da responsabilidade pela segurança do serviço entre o provedor de serviços e a organização deve ser compreendida, com a aplicação dos devidos controles de defesa.	Ao usar serviços de nuvem pública, há uma divisão de responsabilidade pela defesa cibernética entre as questões que são da responsabilidade do provedor e as que permanecem como responsabilidade do cliente. A divisão de responsabilidades depende da natureza do serviço e do modelo de implementação. A organização precisa entender as questões sob sua responsabilidade e implementar as implicações dessa responsabilidade.
Computação em nuvem pública	Compartilhamento de informações sensíveis	Deve-se garantir que os dados cuja transmissão é proibida pelas regulamentações e obrigações da organização não sejam transmitidos aos serviços de nuvem.	Existem dados que a organização não deve transferir para armazenamento ou processamento em serviços de nuvem pública, devido a considerações da regulamentação ou compromissos com terceiros. Antes de transferir dados à nuvem, certifique-se de que não se enquadram nesta categoria.
Proteção de informações	Proteção de informações armazenadas em recursos compartilhados	Deve-se evitar a transmissão não autorizada ou não voluntária de informações por meio de recursos compartilhados do sistema.	A organização deve prevenir e lidar com a transferência de informações não autorizadas por meio de pastas compartilhadas, e-mail, mídia desconectada, etc.

Família	Seção	O controle	Explicação complementar
Segurança da rede	Gestão da sessão no nível da rede	A organização deve utilizar meios tecnológicos para proteger seus serviços de ataques de negação de serviços (DoS, na sigla em inglês).	A proteção contra vários tipos de ataques de negação de serviço deve ser disponibilizada, carregando recursos de computação até que travem, elevando a largura de banda de comunicação ou carregando um site até que ele saia do ar.
Segurança da rede	Confiabilidade da sessão	O serviço de Nomes de Domínio (DNS, na sigla em inglês) deve ser fornecido por um servidor de confiança (tanto dentro como fora da organização).	A organização permitirá a recepção de um Serviço de Nomes de Domínio somente de um servidor interno seguro. Isto ocorre para prevenir rotas de comunicação incorretas (intencional ou acidentalmente) a alvos hosts.
Segurança da rede	Limites da rede	O número de canais externos de comunicação ao sistema deve ser limitado.	A organização reduzirá e unificará os canais de comunicação para assegurar um bom controle sobre as conexões ao sistema.
Segurança da rede	Limites da rede	Por padrão, todo o tráfego da rede deve ser bloqueado, e o tráfego desejado deve ser permitido manualmente por uma regra de exceção.	A organização definirá as regras para filtrar o tráfego da rede e bloquear por padrão qualquer tráfego que não esteja explicitamente determinado como permitido.
Segurança da rede	Limites da rede	Devem ser usados endereços de rede separados (diferentes subredes) para a conexão com sistemas em zonas de segurança diferentes.	A organização definirá que cada subrede terá um intervalo de endereços separado que será publicado no firewall e nos roteadores.

Família	Seção	O controle	Explicação complementar
Controle de acesso	Gestão de usuários	As contas de usuário devem ser configuradas para suportar as funções de negócios da organização.	No mínimo, a conta de um “administrador” deve estar separada da conta de um “usuário”. Os usuários que gerenciem funções de segurança no sistema (como criação de usuário, gestão de acesso e permissões do sistema, ou gestão do sistema de segurança da informação) também devem ser configurados.
Controle de acesso	Gestão de permissões	Os direitos de acesso lógico ao sistema e às informações devem ser definidos e aplicados de acordo com a política de controle de acesso.	O controle de acesso pode ser feito por indivíduo (com base na identidade) ou por função, e seu propósito é controlar o acesso de entidades (usuários ou processos de computador) a objetos (arquivos, registros, dispositivos e mais).
Recursos humanos e conscientização do funcionário	Regras de conduta para funcionários	As regras de conduta devem ser definidas ao trabalhar com os sistemas de informação na organização. Essas regras determinam as áreas de responsabilidade e as regras de uso adequado com ênfase em sistemas sensíveis.	A organização definirá procedimentos comportamentais para o trabalho com os sistemas de informação, e os distribuirá a todos os funcionários.

Família	Seção	O controle	Explicação complementar
Recursos humanos e conscientização do funcionário	Gestão de permissões para o recrutamento/mobilização/saída de férias longas (como licença-maternidade ou licença não remunerada) ou desligamento da organização	Quando um funcionário muda de posição, suas permissões de acesso devem ser revisadas e atualizadas.	Deve ser configurado um processo de atualização relacionado à mobilidade dos funcionários e às permissões modificadas de acordo com a nova posição assumida (remoção de permissões desnecessárias e estabelecimento das permissões requeridas para a nova posição). Formas diferentes de emprego devem ser consideradas, por exemplo, provedores em contraste com funcionários da organização, ou funcionários da organização em contraste com pessoal terceirizado.
Segurança na aquisição e no desenvolvimento	Requisitos de segurança para a aquisição e o desenvolvimento de sistemas	Segurança da cadeia de suprimentos - deve-se exigir que os provedores de serviços cumpram os requisitos, as normas, os padrões e as diretrizes de segurança corporativa.	A organização garantirá que os provedores de serviços cumpram os requisitos de conformidade organizacional, bem como os requisitos regulatórios nos países em que a organização opera.
Defesa física e ambiental	Iluminação de emergência	Deve ser instalada e mantida um sistema de iluminação de emergência automático, que será ativado no caso de falta de energia ou mau funcionamento. O sistema incluirá saídas de emergência e rotas de evacuação na instalação.	

Família	Seção	O controle	Explicação complementar
Defesa física e ambiental	Combate a incêndios	Para preservar os sistemas de informação, devem ser instalados e mantidos sistemas de detecção e extinção de incêndios, que sejam sustentados por uma fonte de energia independente.	
Documentação e monitoramento	Mecanismo da documentação	Deve ser ativado um mecanismo que gere registros de controle sobre incidentes nos sistemas da organização. No mínimo, os incidentes devem ser gravados a partir de sistemas que contêm informações sensíveis dos clientes, de sistemas essenciais para o funcionamento organizacional, e dos sistemas centrais (servidores, componentes de comunicação, aplicativos, bancos de dados, etc.).	A organização garantirá que os sistemas de infraestrutura e os sistemas de aplicativos gerenciem um mecanismo de registro de incidentes. Esses registros devem ser mantidos pelo período de tempo determinado. Os registros de controle conterão informações tais como o tipo de incidente, quando ele ocorreu, a origem do incidente e o nome do usuário. Em qualquer caso, os sistemas que processam informações sensíveis, que fazem parte da infraestrutura essencial da organização, ou aqueles que gerenciam os processos centrais da organização devem ser monitorados.
Documentação e monitoramento	Mecanismo da documentação	Os mecanismos de registro incluirão, no mínimo, informações sobre a natureza da ação realizada, registro da data, origem e destino da ação, identificador do usuário, identificador do processo, falha/sucesso, nome do arquivo misto.	

Família	Seção	O controle	Explicação complementar
Gestão e relatório de incidentes	Tratamento de ciberincidentes e segurança da informação	Os canais de comunicação entre funcionários e supervisores devem ser configurados para relatar incidentes de segurança suspeitos.	A organização aplicará procedimentos que definirão ciberincidentes que precisam ser relatados, determinando o modo de relatá-los.
Continuidade dos negócios	Disponibilidade de recursos	Devem ser feitos back-ups em todos os níveis: usuário, sistema e documentação de sistemas, assegurando sua defesa.	A organização fará back-ups de todas as informações cruciais nos sistemas de informação que sustentem os processos de negócios, garantindo a disponibilidade, integridade e confidencialidade desses back-ups.



Apêndice 2. Lista de exemplos de ameaças e vulnerabilidades

Todos os ciberincidentes podem ser classificados de acordo com a origem do ataque (parte interna, provedor, ou parte externa) e o motivo do ataque (intencional ou acidental). Os seguintes são exemplos de incidentes diferentes, classificados de acordo com esta divisão.

Assim, por exemplo, um arquivo com informações sensíveis pode ser vazado acidental ou intencionalmente por um funcionário da organização, um provedor e/ou um agressor.

Para calcular o **risco** cibernético deve-se ponderar as **vulnerabilidades e ameaças** na organização. Exemplo de vulnerabilidades: falta de um mecanismo de gestão de autorizações, ausência de um mecanismo que bloqueie o computador automaticamente após um período de inatividade, ou uso de um mecanismo fraco de identificação. A ameaça surge quando existe alguém que poderia explorar a vulnerabilidade na organização.

Por exemplo, um funcionário interno que aproveita sus altos privilégios, um agressor que tira partido de um mecanismo de redefinição de senhas fracas, ou um provedor que explora seu acesso a informações sensíveis.

Ao calcular o risco, o grau de motivação e a probabilidade da materialização de uma ameaça devem ser examinados, considerando tanto seu grau de prevalência quanto o grau da sua capacidade de realização (pela exploração de uma ou mais vulnerabilidades).



Gráfico A2.1. Uma parte envolvida no ciberincidente versus o motivo do incidente



Tabela A2.1. Lista de exemplos de ameaças e vulnerabilidades

A causa das ameaças	Maneira de realização/implementação	Vulnerabilidade potencial	Cenários
Agressor remoto	Escuta remota	Telefone IP interno	Ativação remota do microfone em um telefone IP
Agressor remoto	Penetração da internet diretamente na rede da organização	E-mail	Anexar um arquivo infectado à mensagem
Agressor remoto	Penetração da internet diretamente na rede da organização	E-mail	Anexar um link como parte de uma mensagem a um servidor infectado
Agressor remoto	Penetração da internet diretamente na rede da organização	E-mail	Incorporar código hostil em uma organização através de uma mensagem
Agressor remoto	Penetração da internet diretamente na rede da organização	Gateways de comunicação	Exploração de vulnerabilidades (CVE, na sigla em inglês)
Agressor remoto	Penetração da internet diretamente na rede da organização	Gateways de comunicação	Uso da conta de um administrador
Agressor remoto	Penetração da internet diretamente na rede da organização	Serviços da internet	Exploração de vulnerabilidades
Agressor remoto	Penetração da internet diretamente na rede da organização	Serviços da internet	Injetar código hostil

A causa das ameaças	Maneira de realização/implementação	Vulnerabilidade potencial	Cenários
Agressor remoto	Penetração da internet diretamente na rede da organização	Disseminação através do servidor de e-mails corporativos	Exploração de vulnerabilidades
Agressor remoto	Penetração da internet diretamente na rede da organização	Disseminação através do servidor de e-mails corporativos	Uso da conta de um administrador
Agressor remoto	Penetração da internet diretamente na rede da organização	Infectar uma estação na qual o usuário navega	Infectar um computador ao navegar por um servidor infectado
Funcionários	Malícia	Funcionário descontente	Uso de suas permissões legítimas em ações para as quais está autorizado
Funcionários	Malícia	Funcionário descontente	Uso de suas permissões legítimas para realizar ações não autorizadas ou acessar informações não destinadas a ele
Funcionários	Malícia	Funcionário descontente	Uso da conta de outro funcionário para realizar operações autorizadas e não autorizadas
Funcionários	Malícia	Funcionário descontente	Uso de ferramentas de gestão legítimas no computador do funcionário
Funcionários	Acidentalmente	Exposição de um funcionário interno a engenharia social	Infectar o computador de um funcionário através da internet (e-mail, navegação)

A causa da ameaça	Maneira de realização/implementação	Vulnerabilidade em potencial	Cenários
Funcionários	Acidentalmente	Negligência profissional	Criar um link inseguro entre redes diferenciadas
Funcionários	Acidentalmente	Negligência profissional	Fortalecimento inadequado ou insuficiente/incorrecto da segurança e dos meios computacionais
Funcionários	Acidentalmente	Indisciplina	Conectar equipamentos finais infectados a um computador
Funcionários	Acidentalmente	Indisciplina	Link de computador diferenciado à internet

As organizações que precisam responder a ataques avançados deveriam estar preparadas para lidar com técnicas como as que seguem.

01

Desativação de produtos de defesa na organização, como antivírus ou EDR, para posterior execução de *malwares*. O cenário pode ser preparado, entre outros meios, ao:

- reiniciar o computador no Modo Seguro, que está desenhado para restaurar o sistema operacional no caso de mau funcionamento, já que a maioria dos antivírus não são executados nesse modo;
- desativar produtos de segurança pela instalação de softwares de acesso ao kernel e pela exploração de vulnerabilidades desses softwares;
- desativar produtos de segurança usando *malware* que contém código de eliminação de processos;
- evitar produtos de segurança por meio do uso de uma máquina virtual;
- assinar arquivos com *malware* utilizando certificados digitais legítimos;
- uso de *malwares* sem arquivos.

02

Explorar softwares legítimos e ferramentas instalados no computador da vítima por iniciativa própria, ou como parte das ferramentas do sistema operacional (*Living Off the Land*), cujo uso por parte dos agressores não levantaria suspeitas. Lidar com este cenário não é simples por diversos motivos como os que seguem.

- O ataque é executado usando componentes vendidos no mercado e softwares pré-instalados no computador da vítima, sem instalação adicional de arquivos binários pelo agressor.
- Como essas ferramentas costumam ser instaladas por administradores do sistema para realizar atividades legítimas, é difícil bloquear o acesso a elas e identificar ataques. Além disso, mesmo que o ataque seja detectado, é difícil associá-lo com um grupo específico de ataque, porque todos esses grupos usam ferramentas existentes em vez das ferramentas que eles mesmos desenvolveram. Entre outras coisas, este tipo de ataque pode ser realizado com documentos que contenham macros, scripts, ou pela interface de linha de comando, como CLI (na sigla em inglês).

É possível lidar com a exploração de software e ferramentas legítimas nas formas detalhadas

nos capítulos sobre controle da Metodologia de Defesa Cibernética. No entanto, seu direcionamento avançado e sua implementação são necessários na organização. Também é importante definir um conjunto de sinais suspeitos que levarão à investigação de um incidente suspeito. Tais sinais podem incluir a adição de um usuário ao grupo de administração do domínio, a alteração frequente de extensões de arquivos, a tentativa de consultar servidores DNS/NTP que não sejam os servidores oficiais da organização, ou a exclusão de registros.

Extensões sobre tipos comuns de ameaças podem ser encontradas em fontes de referência amplamente aceitas na área, tal como o Apêndice D da norma ISO 27005 ou no projeto MITRE.³ O grau de vulnerabilidade pode ser calculado pelo uso de ferramentas como o padrão CVSS,⁴ que mede uma série de parâmetros.

Os órgãos/entidades/partes que obtêm orientações da Diretoria Cibernética Nacional de Israel poderão receber uma lista mais atualizada de exemplos de ameaças e vulnerabilidades.

3. Mais informações estão disponíveis em: <http://attack.mitre.org/>

4. Para saber mais sobre o CVSS, visite <http://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

Apêndice 3. Banco de controle

O objetivo do banco de controle é centralizar as recomendações de defesa cibernética em várias áreas. O banco de controle será atualizado frequentemente, de acordo com o desenvolvimento da tecnologia e das ameaças derivadas dela.

A estrutura do banco de controle

O banco de controle deve ser representado por uma tabela, contendo as colunas a seguir.

01

Função: uma das cinco áreas principais nas quais a defesa cibernética se divide: identificar, proteger, detectar, responder e recuperar. Estas funções foram estabelecidas de acordo com a estrutura de segurança cibernética (CSF, na sigla em inglês) do NIST.

02

Tema e subtema: estas colunas incluem a família de controle e os capítulos contidos nela. Por exemplo, a família “defesa de nuvem pública” poderia incluir questões secundárias como gestão de alterações na nuvem, operações com uma nuvem híbrida, ou continuidade funcional do trabalho na nuvem.

03

Controle: consiste na própria recomendação de defesa, que deve ser implementada para favorecer o processo de gestão de riscos. Os controles incluem recomendações como a nomeação de um Diretor de Segurança da Informação (CISO), a defesa do navegador ou a realização de atividades de monitoramento.

04

Ênfase na aplicação de controle: visando minimizar o alcance de interpretação. A coluna também pode incluir um detalhamento dos insights e destaques que ajudarão a implementar as recomendações da defesa de modo apropriado e eficaz.

05

Indícios necessários: documentação que o respondente deve apresentar ao solicitante para comprovar que está realmente implementando as recomendações da defesa conforme exigido. Estas medidas apoiam processos de auditoria e podem ajudar a preparar a infraestrutura para credenciamento e certificação.

06

Nível do alvo de controle: para cada recomendação de defesa, foi definido um nível que se move em um eixo de 1 a 4, sendo que 1 representa o controle básico e 4 o controle a ser aplicado onde o potencial de dano é mais significativo. O objetivo desta classificação é servir como uma ferramenta de apoio a

decisões ao considerar a implementação de controles em um alvo de defesa específico, já que nem todos os controles são implementados da mesma forma em todos os processos e sistemas da organização. Além disso, esta divisão ajuda a criar uma diferenciação em favor da proporcionalidade, de modo que as organizações podem começar com a implementação de controles básicos, e posteriormente examinar a implementação de controles mais avançados e complexos.



07

Profundidade de aplicação/controle no nível:

cada controle pode ser aplicado em diferentes níveis de maturação e profundidade. Assim, por exemplo, a implementação de um sistema para prevenir o vazamento de informações pode ser realizada apenas em um nível básico (na compra de um produto e em sua implementação básica), mas também de uma forma integral que leva em conta as limitações da organização, a classificação de informações, a adaptação aos processos de negócios, etc. O controle de nível se move em um eixo que parte do controle de nível básico, indicando normalmente um processo que existe, mas que não é gerenciado e é executado manualmente, e termina com o nível inovador, indicando a implementação do controle de forma gerenciada, documentada, automática, eficiente e eficaz.

08

Colunas adicionais sugeridas: informações sobre mapeamento em contraste com padrões adicionais, acrescentando conteúdo do usuário para realizar o estágio de mapeamento de lacunas.

Uso do banco de controle

O trabalho com o banco de controle envolve dois estágios principais, como segue.

01

O mapeamento de todas as lacunas em contraste com a lista de controles diferentes (com ênfase na coluna de “controle”). Este mapeamento ajuda a entender as questões nas quais a organização não está adequadamente organizada e a obter uma lista de lacunas (análise de lacunas). O processo é de natureza obediente/orientado à conformidade, e o produto é uma lista de “correto/incorreto/irrelevante/parcialmente implementado”.

02

Mapeamento individual de controles em face de ameaças e riscos cruciais em alvos de defesa sensíveis na organização.

Como a implementação de controles é um processo dinâmico que varia de um objetivo de defesa para outro, o nível de controle para certos objetivos de defesa deve ser examinado individualmente. Assim, por exemplo, a capacidade de monitorar e controlar a cadeia de suprimentos e a existência de um

back-up devem ser examinados detalhadamente e em profundidade em determinados objetivos de defesa. Esta abordagem assimila eficazmente a transição de uma perspectiva orientada à conformidade para uma perspectiva baseada em riscos. O uso do banco de controle como uma ferramenta para reduzir riscos e ameaças individuais constitui a realização de seu propósito na visão da administração da organização.

Características únicas do banco de controle na Metodologia de Defesa Cibernética

01

Foco em controles que mais contribuem para a defesa: aqueles que têm a mais alta relação “custo-benefício”.

02

Profundidade de implementação de controles: é possível implementar controles em várias formas, desde sua implementação na organização de forma manual e não sistemática até a implementação integrada apoiada por recursos completos de automação e conheci-

mento profissional atualizado. Para uma implementação eficaz e graduada que ofereça à organização um caminho para melhorar, há várias opções apresentadas ao lado de cada controle em uma profundidade de implementação diferente.

03

Indícios necessários: para garantir que os controles tenham sido adequadamente assimilados na organização, requisitos de ênfase e documentação foram anexados a cada um deles. Estes dados também podem servir como base para regulamentação e/ou credenciamento/certificação de acordo com este método.

04

Classificação e definição de prioridades: para criar uma Metodologia de Defesa Cibernética proporcional, os controles neste documento foram classificados em um eixo que vai de 1 a 4. Os controles de nível 1 são os mais básicos e são exigidos de qualquer organização para cada ativo, enquanto os controles de nível 4 são requeridos apenas para um alvo de defesa cujo potencial de sofrer dano seja 4.

Apêndice 4.

Ferramentas e métodos de implementação do controle contínuo na organização

O controle contínuo é essencial para a organização, porque lhe apresenta um espelho e serve como sua bússola. Este controle permite que a parte da defesa cibernética dentro da organização saiba quais são as lacunas da defesa e que passos devem ser dados para melhorar a situação.

O controle contínuo pode ser executado no nível de conformidade, abordando questões e controles definidos (como o status de conformidade nos controles da Metodologia de Defesa Cibernética), ou medindo riscos, ameaças, prontidão em casos de ataque, entre outros.

Para criar um plano interno de gestão de **controle contínuo**, é necessário definir primeiro uma série de parâmetros de medição. Em seguida, devem ser implementados mecanismos que absorvam os resultados de medição e apresentem a situação atual juntamente com a tendência da organização (é importante que estes mecanismos sejam tão automatizados quanto possível).

Seguem algumas ferramentas e métodos que devem ser implementados na organização para o controle contínuo.

01

Indicadores-chave de desempenho (KPIs, na sigla em inglês). Permitem à organização medir e quantificar o nível de defesa em um momento dado, comparando-o com o histórico de medições, o que possibilitará a análise da tendência. Essas métricas podem analisar, por exemplo:

- o número de usuários que clicaram em um link como parte de uma prática de *phishing*;

- quantidade/porcentagem de servidores e estações de trabalho onde o EDR está instalado, nas quais as atualizações de segurança estão em dia, etc;
- porcentagem de provedores sensíveis para os quais foi realizada uma pesquisa de riscos;
- o tempo médio a partir da publicação de uma atualização de segurança crucial até sua instalação. O tempo médio a partir da chegada de uma advertência no SIEM de um certo nível de gravidade até o início/ fechamento do tratamento Tempo Médio para Identificação (MTTI)/Tempo Médio para Detecção (MTTD);
- porcentagem de controles não implementados a partir da norma, número de cenários/páginas para os quais a organização estava preparada.

02

Indicadores-chave de risco (KRIs, na sigla em inglês). Permitem que a organização monitore o quadro que surge a partir da coleta de dados e perceba a formação do risco. Essas métricas podem analisar uma tendência, mas também medir um desvio de um cenário específico que indica o potencial de risco. Essas métricas podem incluir, por exemplo:

- a quantidade de rastreamentos externos do site;
- a quantidade de relatórios que contêm informações sensíveis que são extraídas do sistema;
- a quantidade de informações copiadas a unidades externas;
- número de tentativas de login fracassadas.



Taxa de alterações e medição

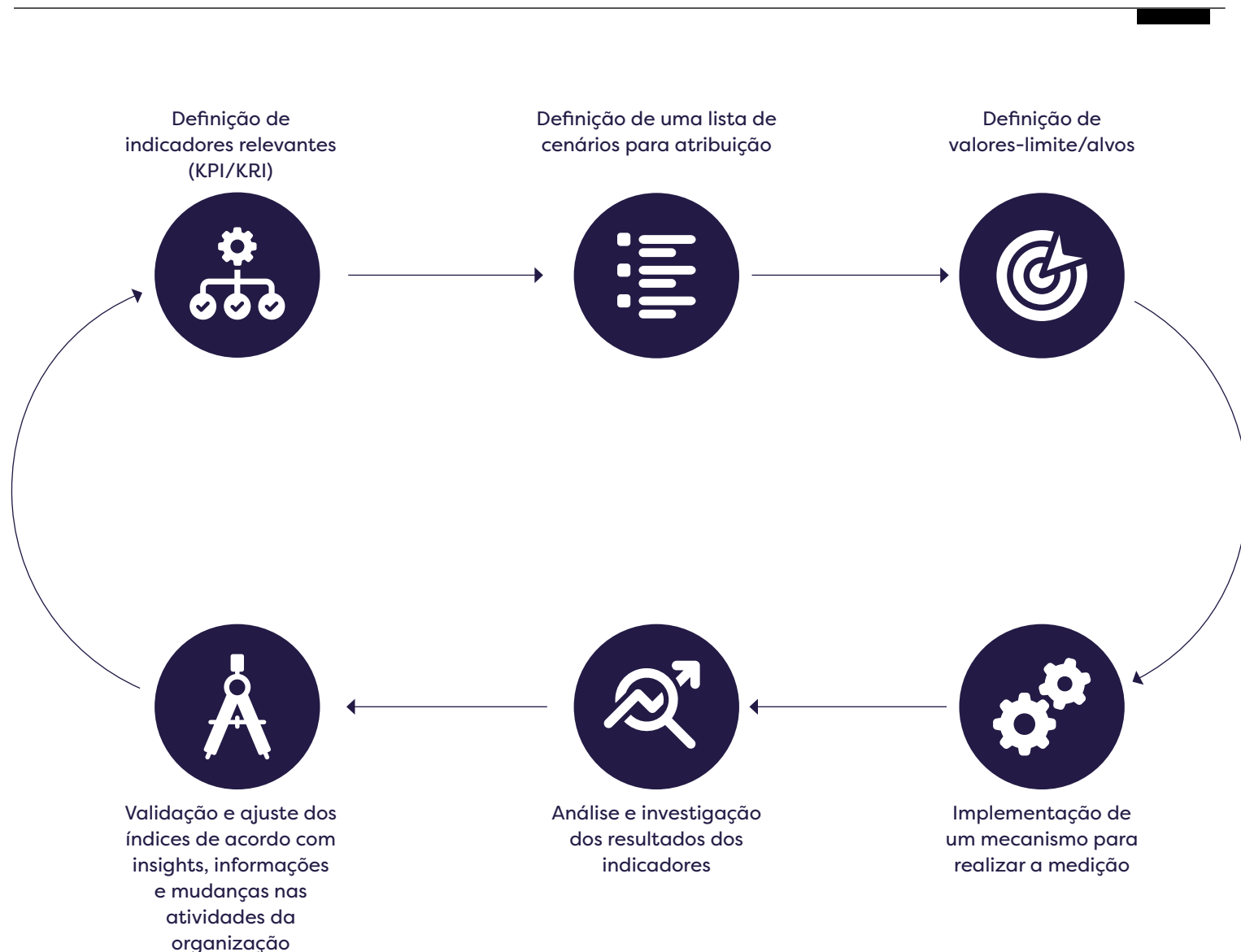
O monitoramento de métricas como KPIs ou KRIs requer que a organização faça uma amostragem de seu status em vários parâmetros em intervalos de tempo definidos. Muitas vezes o processo exige envolvimento manual, bem como trabalho de processamento e análise, portanto, leva tempo. Assim, as métricas podem ser analisadas apenas uma vez por mês ou trimestralmente.

No mundo tecnológico, a taxa de alterações é rápida, por isso, para detectar uma anomalia, algumas das métricas devem ser amostradas uma vez por dia ou mesmo a cada poucas horas; os processos tradicionais de medição não dão resposta ao desafio. Os parâmetros que mudam com frequência precisam de um mecanismo de medição diferente, conhecidos como “Monitoramento de Controle Contínuo”, ou CCM.

A assimilação do conceito de CCM dentro da organização lhe permitirá ver a situação em tempo real e de uma forma que não exija o envolvimento humano.

A organização não pode “esperar” pela seguinte medição de parâmetros, como interfaces abertas (acidental ou intencionalmente), atualizações cruciais que não foram implementadas, a constituição de um firewall de modo tal que ponha a rede em perigo, ou questões sérias de segurança no código do software. Todos esses (e mais) devem ser continuamente monitorados por meio da implementação de tecnologia dedicada.

Gráfico A4.1. O processo de assimilar um mecanismo de CCM na organização



Ênfase na implementação de um programa organizacional de CCM

01

Uma hierarquia organizacional precisa ser definida, incluindo a divisão de autoridade e responsabilidade nessa questão. Por exemplo: como o movimento se encaixa na segunda linha de defesa da organização? O diretor de riscos da organização está integrado na definição e medição das métricas? Há necessidade de responsáveis pela defesa cibernética nas diversas unidades da organização?

02

A plataforma na qual o processo de medição será realizado deve ser definida. As ferramentas de GRC podem oferecer muitos benefícios, embora em alguns casos o processo possa ser gerenciado em outros aplicativos também, como um processador de textos.

03

A demarcação das métricas deve ser analisada, indicando também métricas que “vão além dos limites da organização”, por exemplo, a medição do nível de defesa de provedores externos e subcontratados.

04

Deve-se verificar a existência dos controles e, ao mesmo tempo, desafiar sua eficácia. Este teste deve analisar se um controle que foi implementado de fato enfrenta as ameaças e os riscos que foram assimilados pela organização. Os controles podem ser desafiados com o uso de ferramentas de simulação de ataques, mas também por meio de testes proativos de cenários diferentes. Para isso, pode ser usada uma tabela de “testes eficazes iniciados”, como a que segue.



Tabela A4.1. Verificações reais iniciadas

N.º	Descrição do controle	Resultado desejável em caso de desvio da política aprovada				
		Bloqueio da atividade	Desconexão da rede	Advertência	Reunião de informação/retificação	Outro
1	Ativação/envio de um arquivo de teste (EICAR) usando uma interface aleatória para um ativo cibernético (como e-mail, acesso para compartilhar ou navegação pela página web que contém o arquivo)	X	X	X	X	
2	Vazamento de informações sensíveis ou confidenciais em várias interfaces (por ex., envio a um e-mail externo, upload para o BOX ou impressão)	X		X	X	Informar o gerente de usuários
3	Conexão de um dispositivo de DOC e um modem de celular externo a endpoints aleatórios	X	X	X	X	
4	Remoção/adição de um componente de hardware a um endpoint (por exemplo, memória ou disco rígido)	X	X	X	X	
5	Realização de atividades de rede hostis "silenciosas" (por exemplo, leitura de portas)			X	X	
6	Uso de uma interface de upload de arquivos legítima em um portal interno/externo para carregar um arquivo baseado em formato falso (como um arquivo EXE com valor de PDF do tipo MIME)	X		X	X	

N.º	Descrição do controle	Resultado desejável em caso de desvio da política aprovada				
		Bloqueio da atividade	Desconexão da rede	Advertência	Reunião de informação/retificação	Outro
7	Conexão de um computador que não pertence à organização a uma porta de comunicação aleatória	X	X	X	X	
8	Análise de alguns computadores registrados no diretório corporativo em contraste com o registro do sistema de defesa (como um servidor de gestão de antivírus)				X	
9	Análise da quantidade de usuários registrados no diretório da organização em contraste com o registro dos Recursos Humanos (ou outro departamento da organização)				X	
10	Ativação de uma ferramenta de ataque automático (como o SQLMap) contra um portal da organização (interno/externo)	X		X	X	
11	Análise da configuração de fortalecimento endpoint aleatório em contraste com uma linha de base aprovada de um				X	
12	Análise da lista de atualizações de segurança (patches) em um endpoint aleatório em contraste com uma linha de base aprovada				X	

N.º	Descrição do controle	Resultado desejável em caso de desvio da política aprovada				
		Bloqueio da atividade	Desconexão da rede	Advertência	Reunião de informação/retificação	Outro
13	Instalação/operação de um aplicativo que não foi aprovado para uso na organização	X		X	X	
14	Acesso a um site que viola as políticas permitidas da organização (como um site de compartilhamento de arquivos)	X		X	X	
15	Tentativa de ocultar arquivos que não são permitidos no perfil do usuário	X		X	X	
16	Acesso físico anômalo a arquivos compostos confidenciais			X	X	Chegada de um segurança para interrogatório/verificação de imagem
17	Verificação da atualização da ferramenta de defesa em um endpoint aleatório em contraste com uma linha de base aprovada				X	
18	Criação/modificação/exclusão de uma conta de usuário com privilégios elevados			X	X	
19	Ativação de uma ou mais estações simultaneamente com o mesmo endereço MAC ou IP em complexos/compostos diferentes da organização	X	X	X	X	

N.º	Descrição do controle	Resultado desejável em caso de desvio da política aprovada				
		Bloqueio da atividade	Desconexão da rede	Advertência	Reunião de informação/retificação	Outro
20	Detecção de informações sensíveis/confidenciais/IOC em uma estação de trabalho			X	X	
21	Obtenção de acesso entre redes, mesmo que a política oficial proíba comunicação direta			X	X	
22	Operação de várias SESSÕES com um mesmo endereço IP e um mesmo servidor	X		X	X	
23	Operação de várias SESSÕES com um mesmo endereço IP e vários servidores	X		X	X	
24	Consumo de várias larguras de bandas com um mesmo endereço IP ou vários endereços			X	X	
25	Acesso por SMB (por exemplo) entre estações de trabalho (em vez de acesso a um servidor central)	X		X	X	

Apêndice 5. A árvore doutrinária: uma visão holística da Metodologia de Defesa Cibernética para organizações

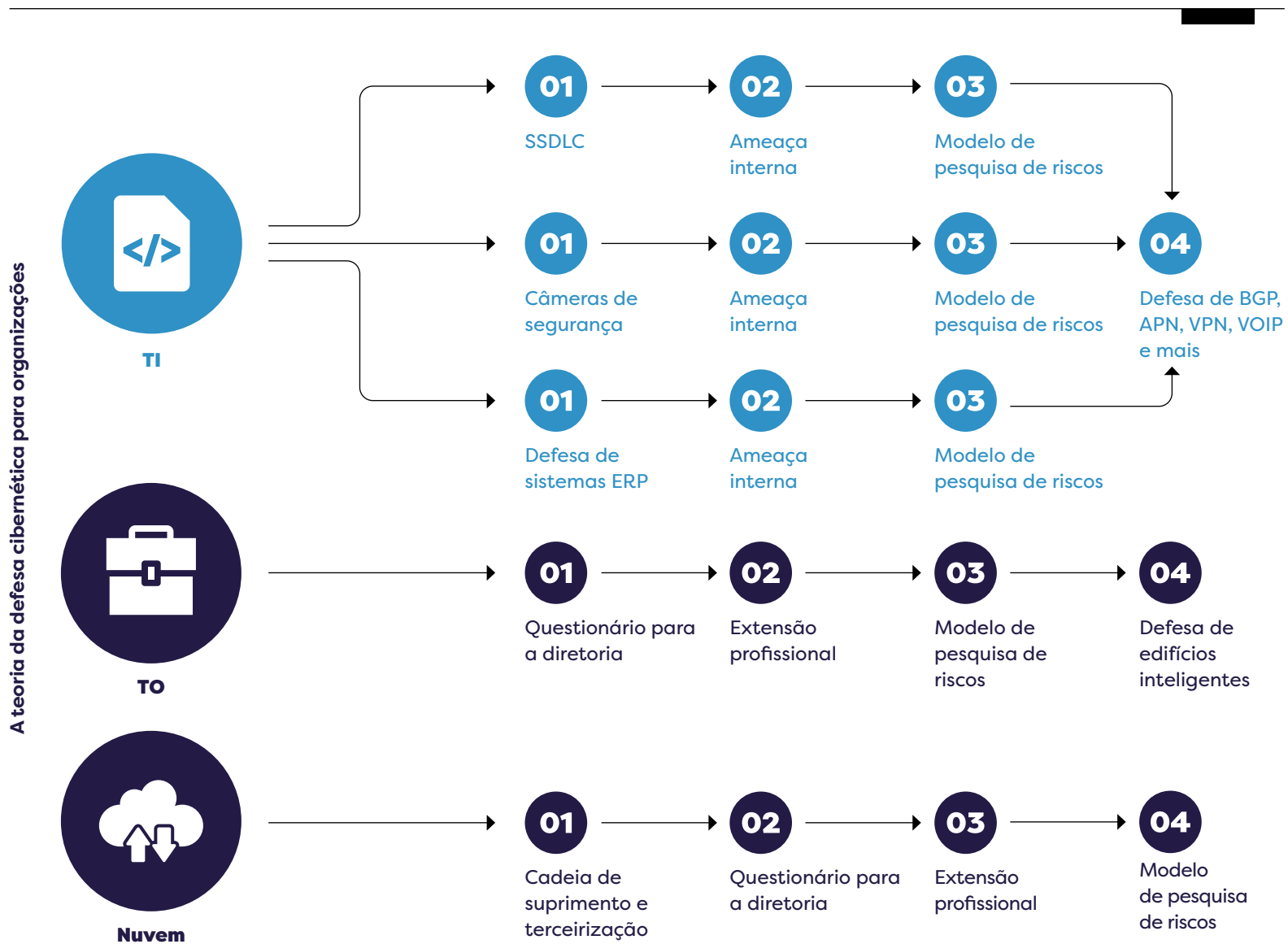
Para ajudar a implementar a Metodologia de Defesa Cibernética e torná-la acessível a diferentes públicos, a Diretoria Cibernética Nacional de Israel desenvolve vários produtos/entregáveis para expandir o conhecimento profissional na área. Além disso, a diretoria fornece ferramentas de apoio que ajudam no processo.

Os produtos/entregáveis desenvolvidos pela Diretoria Cibernética Nacional de Israel estão disponíveis em seu site: https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page. Alguns desses documentos foram traduzidos para o espanhol e fazem parte desta coleção.

Além disso, as informações estão disponíveis no sistema Yuval, uma calculadora exclusiva que permite que qualquer organização em Israel verifique facilmente o nível de sua defesa cibernética.⁵

5. A calculadora Yuval pode ser encontrada em: <http://www.gov.il/he/departments/guides/yuvalrisk>
Atualmente disponível em hebraico.

Gráfico A5.1. A árvore doutrinária: ferramentas e metodologias de defesa que foram criadas pela diretoria cibernética



Observações: SSDLC: ciclo de vida de desenvolvimento de sistema seguro;
BGP: protocolo de gateway de fronteira; APN: nome do ponto de acesso;
VPN: rede privada virtual; VoIP: voz sobre protocolo de internet.

Os produtos de apoio para a implementação da Metodologia de Defesa Cibernética podem se apresentar na hierarquia a seguir.

oferecem ao leitor recomendações individuais de defesa para implementar controles da Metodologia de Defesa Cibernética para uma tecnologia específica, como VPN, VoIP, ou identificação segura.

01

Percepção nacional: com base nela escrevemos a Metodologia de Defesa Cibernética para organizações.

02

Metodologia de Defesa Cibernética: apresenta as diversas questões da defesa no nível básico (por exemplo, monitoramento, conscientização, separação de redes ou gestão da cadeia de suprimento) e os aspectos principais que devem ser considerados na hora de criar um plano de trabalho organizacional. Este documento é a base profissional para realizar uma pesquisa de riscos e criar um plano de trabalho cibernético para a organização.

03

Boas práticas: resultados/produtos que aprofundam as recomendações sobre questões tecnológicas específicas. Estes documentos

04

Extensões profissionais: produtos que apresentam aos leitores o escopo do campo profissional, e lhes fornecem a base profissional ampla para acessar um projeto sobre um tópico específico. Estes produtos não estão concentrados em uma tecnologia específica; em vez disso, apresentam uma variedade de considerações: como abordar a questão; percepções e conselhos que surgiram no diálogo contínuo sobre o assunto com órgãos econômicos; uma visão holística do ramo; e apresentação de um conceito para implementar o tratamento da questão na organização. Exemplos de extensões profissionais disponíveis no site da diretoria: o trabalho do CISO com órgãos de desenvolvimento, defesa de ambientes operacionais, e gestão de riscos da cadeia de suprimentos.

Gráfico A5.2. Produtos de apoio para a implementação da Metodologia de Defesa Cibernética





Apêndice 6. Segurança e privacidade dos dados

A defesa de informações pode ter propósitos diferentes. Por exemplo, prevenir danos à reputação, evitar vazamento de informações comerciais, ou a fuga de informações privadas.

Embora aos olhos dos órgãos/entidades envolvidos na defesa da computação a defesa seja normalmente a mesma (como criptografar um arquivo ou estabelecer princípios estritos para o controle de acesso), **a finalidade**, por outro lado, pode ser diferente.

O direito à privacidade foi reconhecido em uma Lei Básica: Dignidade e liberdade humanas, em várias leis (principalmente a Lei de Proteção da Privacidade), bem como em convenções internacionais. A Lei de Proteção da Privacidade inclui uma série de princípios fundamentais. Um deles é o **princípio de consentimento**, que expressa o controle do indivíduo sobre as informações que lhe

dizem respeito. É ele que decide que informações serão divulgadas e para quem.

Esse princípio está refletido, entre outros, na Seção 1 da Lei de Proteção da Privacidade, que afirma que **“uma pessoa não deve violar a privacidade de outra sem seu consentimento”**. De acordo com a Lei de Proteção da Privacidade, o consentimento nesse contexto deve ser “informado”, ou seja, dado somente depois que a pessoa entender o significado de dar seu consentimento e suas consequências.

Outro princípio fundamental é o da **proximidade da meta**. Segundo este princípio, que é regulamentado sob as Seções 2 (9) e 8 (b) da Lei de Proteção da Privacidade, as informações podem ser usadas somente de acordo com a finalidade para a qual foram coletadas. O uso das informações para qualquer finalidade diferente constitui uma invasão de privacidade.

A Lei de Proteção da Privacidade e as regulamentações por ela promulgadas também estipulam várias obrigações relacionadas ao registro de bancos de dados e à maneira como eles são protegidos. Entre outras coisas, há uma obrigação de examinar a necessidade de retenção adicional de informações, de acordo com a finalidade para a qual foram coletadas.

A Lei de Proteção da Privacidade também se refere aos **direitos do Titular dos Dados**. De acordo com a seção 11 da lei, o Titular dos Dados deve ser notificado sobre a intenção

de coletar as informações e a finalidade de seu uso. Também deve ser informado se tem a obrigação legal de fornecê-las ou se pode se recusar a fazê-lo. A Seção 13 da Lei concede ao Titular dos Dados o direito de revisar as informações que lhe dizem respeito. A Seção 14 lhe concede o direito de exigir sua correção nas circunstâncias apropriadas.

Porém, como todos os direitos, o direito da privacidade não é absoluto. Pode haver circunstâncias nas quais outros interesses justifiquem sua violação específica. Este conceito é regulamentado, entre outros, nas defesas estabelecidas na Seção 18 da Lei de Proteção da Privacidade. No entanto, tal infração deve ser realizada de acordo com o objetivo das disposições da lei, obedecendo aos princípios gerais de ação de razoabilidade e boa-fé; e no caso de órgãos públicos, também deve cumprir o requisito de proporcionalidade.

Em geral, a defesa cibernética é uma **ação legítima** que não envolve nenhuma invasão excepcional de privacidade.

No entanto, sua implementação real deve ser realizada com a profunda consideração dos aspectos de privacidade e conformidade com princípios aceitos, tais como *Security by Design* (**Segurança desde a concepção**), *Privacy by Design* (**Privacidade desde a concepção**) e *Threat Informed Defense* (**Defesa informada sobre ameaças**). Esses

princípios exigem que o CISO tenha uma compreensão profunda do processo tecnológico. Ele também deve saber como encontrar o **equilíbrio certo entre os diferentes interesses** para que suas recomendações à administração da organização permitam a tomada de decisões informadas.

A Metodologia de Defesa Cibernética enfatiza que é importante que o CISO envolva o **consultor jurídico** da organização já no estágio de iniciação e caracterização do plano de trabalho para reduzir as disparidades de segurança. Posteriormente, ele deve ser integrado aos principais nós do ciclo de vida das informações dos negócios, dos processos de negócios e de vários ativos cibernéticos. Assim, por exemplo, o envolvimento do consultor jurídico é necessário já no estágio do **mapeamento de requisitos da lei, da regulamentação, dos requisitos contratuais e necessidades comerciais** que a organização deva cumprir. Todos eles formam a base para a existência do processo de gestão de riscos e a conformidade da administração com as obrigações aceitáveis, como os procedimentos de devida diligência.

Também é importante que o consultor jurídico da organização seja membro permanente dos **comitês de direção**, como o Comitê de Defesa da Informação e o de Defesa Cibernética. Além disso, deve estar envolvido nos **processos de emprego e processos de contratação** com vários órgãos/entidades/partes da cadeia de suprimentos.

Adicionalmente, a estrutura de controle da Metodologia de Defesa Cibernética oferece ao CISO **ampla liberdade de ação**. Isto lhe permite reduzir o nível de riscos a um valor aceitável e, ao mesmo tempo, minimizar a invasão de privacidade.

A Metodologia de Defesa Cibernética enfatiza que a organização deve usar **círculos de segurança independentes** para lidar com as diversas ameaças (como o abuso de privilégios legítimos) e que a tomada de decisões deve estar baseada em evidências. Como resultado, além da capacidade de obter uma imagem realista da situação da segurança na organização (Postura de segurança), será possível aumentar a probabilidade de que ações que violam a privacidade sejam executadas somente diante de necessidades reais.

A Metodologia de Defesa Cibernética também enfatiza a importância de **usar processos de automação e orquestração**. Isso **reduz a necessidade do envolvimento humano** nos processos operacionais e de defesa e, portanto, a probabilidade de erro humano. Ao mesmo tempo, diminui o nível de exposição dos diversos órgãos às informações pessoais. Por exemplo, ao adotar a ontologia MITRE ATT&CK, a organização poderá usar soluções de automação avançadas para o controle contínuo e permanente e a execução de processos de resposta, de modo que o envolvimento manual humano só será necessário em casos excepcionais.

Além disso, a Metodologia de Defesa Cibernética **estabelece a necessidade de tomar atitudes proativas** de defesa para preservar as informações. Isto além de manter os **recursos eficazes para lidar** com eventos de vazamento de informações, adquirindo a capacidade de remover informações que vazaram para a internet e a Darknet.

Em conclusão, pode-se ver que o CISO é uma parte significativa na proteção das informações e da privacidade, e que ele deve aproveitar as diversas entidades dentro da organização para maximizar o nível de defesa.

Integração de atividades de defesa para melhorar o nível de proteção da privacidade na organização

Os controles da Metodologia de Defesa Cibernética são incorporados em uma estrutura, que inclui aspectos de identificação, defesa, detecção, resposta e recuperação. Por meio da implementação das recomendações de defesa cibernética e segurança de informações, aspectos que ajudam na defesa da privacidade estão, em alguns casos, entrelaçados nos próprios controles.

Apêndice 7. Um conceito avançado de defesa para organizações

O conceito de defesa necessário para abordar ameaças avançadas inclui abordagens avançadas.

O uso dessas abordagens ajudará a organização a alcançar recursos avançados, como validação e engano a fim de ganhar tempo, esgotar o agressor e até dissuadir possíveis agressores. Estes princípios podem incluir, entre outros:

- **negação e engano (D&D, na sigla em inglês);**
- **mascaramento e ofuscação;**
- **resistência à adulteração e prova de adulteração;**
- **defesa contra silêncio;**
- **caça a ameaças;**
- **monitoramento contínuo;**
- **diversidade/defesa de alvos móveis (MTD, na sigla em inglês).**

Os princípios da defesa avançada podem ser aplicados por meio da adoção de estruturas e projetos de trabalho, como o ataque MITRE ou a abordagem/modelo CYBER KILL CHAIN, e por meio da divisão das percepções em processos e rotinas de defesa dentro da organização.

Eis aqui alguns exemplos de componentes de um conceito organizacional e exemplos de sua implementação em rotinas de defesa.

A base para a implementação de um conceito avançado é o profissionalismo dos responsáveis pela proteção cibernética na organização. As organizações que pretendem adotar esses conceitos devem investir em treinamento avançado e contínuo dos profissionais relevantes.



Tabela A7.1. Componentes de um conceito organizacional e exemplos de implementação em rotinas de proteção

Componente	Explicação	Propósito	Exemplos
Esgotamento	Erosão gradual e contínua da capacidade de combate do agressor por meio de danos cumulativos a suas unidades/recrutadas, seus meios e seu espírito (de acordo com o glossário das Forças de Defesa de Israel).	Mudança da equação de viabilidade do atacante em relação ao corpo defensor. Erguer os muros para que o corpo defensor não seja o alvo preferido para atingir o objetivo do ataque.	A execução de ações proativas com alta frequência para verificar a integridade da superfície de ataque interna/externa da organização pode favorecer a detecção, identificação e tratamento de pontos fracos antes que sejam vulnerados. Como resultado, um atacante em potencial pode concluir que o uso de métodos de ataque convencionais (como <i>Webshell</i>) contra a organização pode não ser suficientemente eficaz. Isso vai obrigá-lo a desenvolver meios alternativos de ataque (uma ação que aumentará o custo do ataque e o prolongará) ou a apontar a outros alvos mais acessíveis.
Conscientização da situação cibernética	Capacidade de oferecer uma boa compreensão do que está acontecendo no ciberespaço e suas implicações para a continuidade do funcionamento da organização/economia.	Criação de uma infraestrutura de tomada de decisões com base em uma compreensão da situação das principais ameaças aos principais ativos da organização.	O sistema de defesa cibernética nas organizações muitas vezes sofre de uma falta de recursos constante. Uma organização educada para entender quais são os seus tesouros e quais são os mais recentes vetores de ataque que um possível agressor poderia usar será capaz de priorizar seus esforços de defesa mais corretamente.
Dissuasão	Uma ação ou processo de ameaça, que impede o agressor de executar ações por medo de suas consequências. A dissuasão dá ao agressor a sensação de que uma ameaça plausível paira sobre ele, e que ele não tem como confrontar essa ameaça. Vale notar que a capacidade de criar dissuasão depende da existência da autoridade jurídica adequada, e portanto, a capacidade da organização de dissuadir nesse caso estará baseada principalmente no uso de instrumentos jurídicos e financeiros. Para manter a confiabilidade da dissuasão, a organização deve certificar-se de ativar esses dispositivos quando necessário.	Reduzir a motivação de um oponente de atacar a organização.	Quando um usuário executa uma ação suspeita de ser uma tentativa de reunir informações antes de um ataque, a mensagem aparece na tela: "Você pode estar executando uma ação definida como ilegal; a partir deste momento, todas as suas ações são monitoradas e documentadas, e a organização reserva-se o direito de responder por vários meios". A dissuasão pode ser aplicada de modo mais "suave", por meio de acordos legais ou <i>Hack Back</i> (<i>hackear de volta o hacker</i>). Em todo caso, é obrigatório acompanhar essa atividade com assessoramento jurídico, devido aos riscos que lhe são inerentes.
Prevenção e fraude (D&D: negação e engano)	Usar vários meios e métodos para enganar o agressor, e inclusive obter informações valiosas. Porém, o sucesso real depende da capacidade de combinar os meios e os métodos de trabalho para que se adaptem ao ambiente de produção existente ou ao que o agressor acredita que existe.	Ganhar tempo a partir do momento em que o ataque começa até sua execução, para aprender os cursos de ação do oponente, e receber advertências antecipadas sobre tentativas de ataques direcionados. Além de atrasar e aprender sobre o agressor, as ferramentas de ENGANO possibilitam a MITIGAÇÃO (ou seja, ISOLAMENTO ou BLOQUEIO) quando se conectam com ferramentas existentes na organização (FW, AV, EDR, NAC e outras).	Esta família inclui, por exemplo, o uso de um <i>Honeybot</i> , <i>Emulador</i> , <i>Honeytokens</i> , <i>Honeynets</i> , desinformação e <i>Deepfake</i> . Todos esses podem ser implementados por vários métodos, tais como: <i>HONEYPOT FULL OS / HONEYPOT EMULATION / HONEYDOCS</i> Também é possível combinar ações a aparências no nível do processo.



Prezados gerentes e especialistas em segurança da informação e proteção cibernética:

O ciberespaço é o resultado dos avanços tecnológicos, da conectividade e da conexão global com a internet. A crescente dependência dele traz consigo uma série de inovações tecnológicas e enormes desenvolvimentos para as pessoas e seu ambiente. Entretanto, também cria um espaço de ameaças que afeta a continuidade dos negócios, a integridade dos processos de produção e a confidencialidade das informações das organizações.

Os ciberataques podem causar danos às organizações, incluindo a interrupção dos processos de produção, prejuízos econômicos e prejuízos à reputação. O Estado de Israel está fazendo um esforço nacional de proteção cibernética no espaço civil. A Metodologia de Defesa Cibernética para Organizações é uma das fases do Conceito de Defesa Nacional, que consiste em diferentes camadas de proteção para a economia israelense e sua continuidade operacional.

Essa metodologia abrange a organização como um todo e permite aumentar seu nível de resiliência por meio da implementação contínua de processos, métodos e produtos voltados para a proteção. Consequentemente, sua implementação aumentará sua resiliência e resistência a ciberataques.

O ciberespaço é um reino de oportunidades em termos de progresso tecnológico, conectividade, integração e conectividade global com a internet. Mas também é um terreno de ameaças e riscos. Os ciberataques podem prejudicar as organizações e infligir prejuízos econômicos e de reputação significativos. Para que uma organização esteja preparada para se defender contra ameaças cibernéticas, deve dominar uma ampla gama de especializações: tecnológicas, organizacionais e de processos. A lista de capítulos apresentada abaixo reflete o estado da coleção no momento da publicação deste documento.

Volume A: Uma abordagem metodológica

- A.01 Metodologia de defesa cibernética para organizações - Versão 1.0
- ▶ A.02 Metodologia de defesa cibernética para organizações - Versão 2.0
- A.03 Uso de serviços em nuvem: adendo à metodologia de defesa cibernética para organizações
- A.04 Recomendações de defesa: a ameaça interna
- A.05 Preparação da organização para uma crise cibernética
- A.06 Cadeia de suprimentos
- A.07 Perguntas de orientação para formuladores de políticas cibernéticas
- A.08 Recomendações de cibersegurança e redução de riscos cibernéticos para pequenas empresas
- A.09 Prática cibernética: criação e edição de exercícios de cibersegurança para organizações
- A.10 Gestão de riscos cibernéticos em ambientes de tecnologia operacional (TO)
- A.11 Modelo de avaliação de riscos no varejo
- A.12 Prática cibernética: criação de planos de conscientização para organizações

Volume B: Uma abordagem técnica

Volume C: Desenvolvimento de software seguro

