GUIA DE APERFEIÇOAMENTO DA SEGURANÇA CIBERNÉTICA PARA INFRAESTRUTURA CRÍTICA

Versão 1.1

https://doi.org/10.6028/NIST.CSWP.04162018pt

O Conselho Empresarial Brasil-EUA da Câmara de Comércio dos EUA oferece esta tradução à comunidade de língua portuguesa, não sendo uma tradução oficial do governo norte-americano, porém traduzido com permissão do Instituto Nacional de Padrões e Tecnologia (NIST). A versão oficial deste documento é a versão em inglês, disponível no https://doi.org/10.6028/NIST.CSWP.04162018.

U.S. CHAMBER OF COMMERCE

A Câmara de Comércio dos EUA é a maior federação empresarial do mundo, representando os interesses de mais de 3 milhões de empresas de todos os portes, setores e regiões, além de câmaras estaduais e locais e associações industriais.

Brazil - U.S. Business Council

O Conselho é parte da Câmara de Comércio dos EUA, baseada em Washington, D.C. Com mais de 95 empresas associadas, o Conselho trabalha há mais de quatro décadas para a promoção de um estreito diálogo entre os governos e empresas norte-americanas e brasileiras que investem e produzem no Brasil. Juntas, as duas entidades trabalham para fortalecer a relação bilateral, melhorar o ambiente de negócios dos dois países e contribuir para o desenvolvimento sustentado de ambas as nações.

Nota aos Leitores sobre a Atualização

A versão 1.1 deste Guia de Segurança Cibernética refina, esclarece e aprimora a versão 1.0 que foi publicada em fevereiro de 2014. Ele reúne comentários recebidos nas duas propostas da Versão 1.1.

A versão 1.1 deve ser adotada por usuários antigos e iniciantes do Guia. Os usuários antigos devem conseguir colocar a versão 1.1 em prática com pouca ou nenhuma dificuldade; a compatibilidade com a Versão 1.0 foi levada em consideração.

A tabela abaixo resume as alterações entre a versão 1.0 e a versão 1.1.

Tabela NTR-1 - Resumo das alterações entre a Versão 1.0 e a Versão 1.1 do Guia

Atualização	Descrição da Atualização
Esclareceu que termos como "*compliance*" podem ser confusos e ter um significado muito diferente para os vários *stakeholders* do Guia.	Maior clareza de que o Guia tem utilidade como estrutura e linguagem para organizar e apresentar *compliance* com os próprios requisitos de segurança cibernética de uma organização. No entanto, a variedade de formas pelas quais o Guia pode ser utilizado por uma organização significa que frases como "*compliance* com o Guia" podem ser confusas.
Uma nova seção sobre autoavaliação	A Seção 4.0 Autoavaliação do Risco de Segurança Cibernética através do Guia foi incluída para explicar como o Guia pode ser utilizado por organizações para que elas possam entender e avaliar o risco de segurança cibernética que sofrem, inclusive por meio do uso de medições.
Ampliou a explicação quanto à utilização do Guia para fins de Gerenciamento de Riscos na Cadeia de Suprimentos	Uma seção 3.3 Informar os *stakeholders* sobre os Requisitos de Segurança Cibernética mais ampla ajuda os usuários a entender melhor o SCRM Cibernético (Gerenciamento de Riscos na Cadeia de Suprimentos Cibernéticos), ao passo que uma nova Seção 3.4 Decisões de Compra destaca o uso do Guia na compreensão do risco relacionado a produtos e serviços comerciais prontos para o

Cibernéticos	consumo. Critérios adicionais do SCRM Cibernético foram adicionados aos Níveis de Implementação. Finalmente, uma categoria de Gerenciamento de Riscos na Cadeia de Suprimentos, incluindo várias Subcategorias, foi adicionada à Estrutura Básica.
Melhorias nos processos de autenticação, autorização e verificação de identidade	A linguagem da Categoria de Controle de Acesso foi aperfeiçoada para melhorar os processos de autenticação, autorização e verificação de identidade. Isso incluiu a adição de uma Subcategoria para cada Autenticação e Verificação de Identidade. Além disso, a Categoria foi renomeada para Gerenciamento de Identidade e Controle de Acesso (PR.AC) para representar melhor o escopo da Categoria e Subcategorias correspondentes.
Melhor explicação da relação entre os Níveis de Implementação e as Avaliações	Adicionou terminologia para a Seção 3.2 *Elaboração ou Melhoria de um Programa de Segurança Cibernética* a respeito do uso de Níveis de Implementação. Atualizou a terminologia nos Níveis de Implementação para refletir a integração das considerações do Guia nos programas organizacionais de gerenciamento de risco. Os conceitos acerca do Nível de Implementação também foram refinados. A Figura 2.0 foi atualizada para incluir ações dos Níveis de Implementação.
Estudo sobre a Divulgação de Vulnerabilidade Coordenada	Foi incluída uma Subcategoria relacionada ao ciclo de vida da divulgação de vulnerabilidade.

Assim como na Versão 1.0, os usuários da Versão 1.1 são incentivados a personalizar o Guia para aumentar o valor organizacional de cada usuário.

Agradecimentos

Esta publicação é resultado de um esforço colaborativo contínuo envolvendo a indústria, o meio acadêmico e o governo. O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST, sigla em inglês) lançou este projeto reunindo organizações e indivíduos do setor privado e público no ano de 2013. Este *Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica* foi publicado em 2014 e revisado em 2017 e 2018. Ele contou com a realização de oito oficinas públicas, respondeu a várias Solicitações de Comentários ou Informações, e milhares de interações diretas com *stakeholders* de todos os setores dos Estados Unidos, juntamente com diversos setores de todo o mundo.

O motivo para alterar a versão 1.0 e as alterações que aparecem nesta versão 1.1 foram baseadas em:

- Feedback e perguntas frequentes realizadas ao NIST desde o lançamento da Versão 1.0 do Guia;
- 105 respostas ao pedido de informações (RFI) de dezembro de 2015, *Opiniões sobre o Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica* ;
- Mais de 85 comentários em uma segunda proposta da Versão 1.1 apresentada em 5 de dezembro de 2017 ;
- Mais de 120 comentários na primeira proposta da Versão 1.1 em 10 de janeiro de 2017; e
- Colaboração de mais de 1.200 participantes nos grupos de trabalho do Guia nos anos de 2016 e 2017 .

Além disso, o NIST lançou a Versão 1.0 do Guia de Segurança Cibernética com um documento complementar, o *Roteiro do NIST para Aperfeiçoar a Segurança Cibernética da Infraestrutura Crítica*. Este Roteiro destacou as principais "áreas de aperfeiçoamento" que careciam de desenvolvimento, harmonização e colaboração. Por meio de esforços do setor público e privado, algumas áreas de aperfeiçoamento avançaram o suficiente para serem incluídas neste Guia Versão 1.1.

O NIST reconhece e agradece a todos aqueles que contribuíram para este Guia.

Este Guia foi traduzido por cortesia da Câmara de Comércio dos EUA e do Conselho Empresarial Brasil-EUA. Esta não é uma tradução oficial do governo dos EUA. Avaliado por Leader Translations, Ins.

Síntese

Os Estados Unidos dependem de um funcionamento confiável por parte da infraestrutura crítica. As ameaças de segurança cibernética exploram o aumento da complexidade e da conectividade de sistemas de infraestrutura críticas, colocando em risco a segurança, a economia, a segurança pública e a saúde da nação. Semelhante aos riscos financeiros e de reputação, o risco de segurança cibernética afeta o resultado final de uma empresa. Pode elevar os custos e afetar a receita. Esse risco pode prejudicar a capacidade de uma organização de inovar, e de conquistar e manter clientes. A segurança cibernética pode ser um componente importante e amplificador do gerenciamento geral de riscos de determinada organização.

Para melhor tratar esses riscos, a Lei de Aprimoramento da Segurança Cibernética de 2014[1] (CEA, em inglês) atualizou a função do Instituto Nacional de Padrões e Tecnologia (NIST, em inglês) de modo a incluir a identificação e o desenvolvimento de diretrizes de risco de segurança cibernética para uso voluntário de proprietários e operadores de infraestrutura crítica. Por meio da CEA, o NIST deve identificar "uma abordagem priorizada, flexível, reproduzível, econômica e baseada no desempenho, incluindo medidas e controles de segurança da informação que possam ser adotados voluntariamente pelos proprietários e operadores de infraestrutura crítica para ajudá-los a identificar, avaliar e gerenciar os riscos cibernéticos". Isso deu forma ao trabalho anterior do NIST para o desenvolvimento da Versão 1.0 do Guia sob Decreto n.º 13636, "Aperfeiçoando a Segurança Cibernética da Infraestrutura Crítica" (fevereiro de 2013), e forneceu orientações para um aprimoramento futuro do material. O Guia, que foi desenvolvido a partir do Decreto n.º 13636 e continua a ser aperfeiçoado de acordo com a CEA, usa uma linguagem comum para combater e gerenciar os riscos de segurança cibernética de maneira econômica com base nas necessidades comerciais e organizacionais, sem impor requisitos regulamentares adicionais às empresas.

O Guia se concentra no uso de indicadores de negócios para orientar as atividades de segurança cibernética e considerar os riscos de segurança cibernética como parte dos processos de gerenciamento de riscos da organização. Este Guia consiste em três partes: a Estrutura Básica, os Níveis de Implementação e as Avaliações da

[1] Consulte 15 USC § 272 (e) (1) (A) (i). A Lei de Melhoria da Segurança Cibernética de 2014 (S.1353) tornou-se a lei pública n.o113-274 em 18 de dezembro de 2014 e pode ser acessada em: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Estrutura. A Estrutura Básica é um conjunto de atividades, resultados e referências informativas de segurança cibernética que são comuns entre os setores e a infraestrutura crítica. Elementos da Estrutura fornecem orientação detalhada para o desenvolvimento de Avaliações organizacionais específicas. Por meio do uso de Avaliações, o Guia ajudará uma organização a alinhar e priorizar suas atividades de segurança cibernética de acordo com seus requisitos do negócio ou de sua missão, suas tolerâncias a riscos e seus recursos. Os Níveis de Implementação fornecem um mecanismo para as organizações visualizarem e compreenderem as características de sua abordagem para gerenciar os riscos de segurança cibernética, o que as ajudará a estabelecer prioridades e atingir seus objetivos no que tange à segurança cibernética.

Embora este documento tenha sido desenvolvido para aperfeiçoar o gerenciamento de riscos de segurança cibernética em infraestruturas críticas, o Guia pode ser usado por organizações de qualquer setor ou pela sociedade. O Guia permite que as organizações (independentemente do tamanho, grau de risco de segurança cibernética ou sofisticação de segurança cibernética) apliquem os princípios e as boas práticas de gerenciamento de riscos para melhorar a segurança e a resistência.

O Guia fornece uma estrutura de organização comum para várias abordagens à segurança cibernética, reunindo padrões, diretrizes e práticas que estão funcionando de forma eficaz hoje em dia. Além disso, por referenciar padrões mundialmente reconhecidos de segurança cibernética, o Guia pode servir como modelo para cooperação internacional no fortalecimento da segurança cibernética em infraestruturas críticas, bem como em outros setores e comunidades.

O Guia oferece uma maneira flexível de lidar com a segurança cibernética, incluindo o efeito da segurança cibernética nas dimensões físicas, cibernéticas e referentes a pessoas. É aplicável a organizações que dependem de tecnologia, seja seu foco em segurança cibernética principalmente na tecnologia da informação (TI), sistemas de controle industrial (ICS), sistemas ciber-físicos (CPS) ou em dispositivos conectados de forma mais generalizada, incluindo a Internet das Coisas (IoT). O Guia pode auxiliar as organizações a lidar com a segurança cibernética, pois ela afeta a privacidade de clientes, funcionários e outras partes.
Além disso, os resultados do Guia servem como alvos para atividades de desenvolvimento e aprimoramento dos recursos humanos.

O Guia não é uma abordagem única e exclusiva para gerenciar o risco de segurança cibernética para infraestruturas críticas. As organizações continuarão a ter seus próprios riscos — diferentes ameaças, diferentes vulnerabilidades e diferentes tolerâncias de risco. Há variação também sobre como elas customizam

as práticas descritas no Guia. As organizações podem determinar quais atividades são importantes para a entrega de serviços críticos e podem priorizar investimentos para aumentar o impacto de cada dólar gasto. Por fim, o Guia visa a reduzir e gerenciar melhor os riscos de segurança cibernética.

Para atender às necessidades específicas de segurança cibernética inerentes a cada organização, há uma grande variedade de formas de utilizar o Guia. A decisão sobre como aplicá-lo é responsabilidade da organização implementadora. Por exemplo, uma organização pode optar por utilizar os Níveis de Implementação do Guia para articular as práticas de gerenciamento de risco previstas. Uma outra organização pode usar as cinco funções da Estrutura Básica para analisar todo o seu portfólio de gerenciamento de riscos. Essa análise pode ou não contar com orientações complementares mais detalhadas, como, por exemplo, catálogos de controles. Às vezes há discussão sobre "*compliance*" com o Guia, sendo que o mesmo funciona como uma estrutura e linguagem para organizar e apresentar o programa de *compliance* de acordo com os requisitos de segurança cibernética da própria organização. No entanto, a gama de maneiras pelas quais o Guia pode ser usado por uma organização significa que frases como "*compliance* com o Guia" podem ser confusas e significar algo muito diferente para os vários *stakeholders*.

O Guia é um documento vivo e continuará a ser atualizado e aperfeiçoado a partir de feedback dado pela indústria sobre sua aplicação. O NIST continuará coordenando junto ao setor privado e agências governamentais de todos os níveis. À medida que o Guia é colocado em prática, outras lições aprendidas serão incluídas em versões futuras. Isso garantirá que o Guia atenda às necessidades dos proprietários e operadores de infraestrutura crítica em um ambiente dinâmico e desafiador repleto de novas ameaças, riscos e soluções.

Os próximos passos para aperfeiçoar a segurança cibernética da infraestrutura crítica em nosso país são o uso ampliado e mais eficiente deste Guia referencial, aliado ao compartilhamento das boas práticas — fornecer orientações a organizações individuais ao mesmo tempo que se melhora a segurança cibernética da infraestrutura crítica da nação, da economia e da sociedade em geral.

Índice

Lista de Figuras

Lista de Tabelas

1.0 Introdução ao Guia

Os Estados Unidos dependem de um funcionamento confiável de sua infraestrutura crítica. As ameaças de segurança cibernética exploram o aumento da complexidade e da conectividade de sistemas de infraestrutura críticas, colocando em risco a segurança da nação, da economia, e da saúde e segurança pública. Semelhante aos riscos financeiros e de reputação, o risco de segurança cibernética afeta o resultado final de uma empresa. Isso pode elevar os custos e afetar sua receita. Pode prejudicar a capacidade de uma organização de inovar, e de conquistar e manter clientes. A segurança cibernética pode ser um componente importante e amplificador do gerenciamento geral de riscos de uma organização.

Para fortalecer a resiliência desta infraestrutura, a Lei de Aprimoramento da Segurança Cibernética de 2014[2] (CEA, em inglês) atualizou o papel do Instituto Nacional de Padrões e Tecnologia (NIST) para "facilitar e apoiar o desenvolvimento de" diretrizes sobre risco de segurança cibernética. Por meio do CEA, o NIST deve identificar "uma abordagem priorizada, flexível, reproduzível, econômica e fundamentada no desempenho, incluindo medidas e controles de segurança da informação que possam ser adotados voluntariamente pelos proprietários e operadores de infraestrutura crítica para ajudá-los a identificar, avaliar e gerenciar os riscos cibernéticos". Isso oficializou o trabalho anterior do NIST desenvolvendo a Versão 1.0 do Guia sob Decreto n.º 13636, "Aperfeiçoando a Segurança Cibernética da Infraestrutura Crítica", publicado em fevereiro de 2013[3], e forneceu orientações para aperfeiçoamento futuro do Guia.

A Infraestrutura crítica[4] tem sua definição no *US Patriot Act* de 2001[5] como "sistemas e ativos, sejam eles físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante sobre a segurança econômica nacional, saúde e segurança pública nacional, ou na combinação de qualquer uma dessass áreas." Devido às crescentes pressões de ameaças externas e internas, as organizações responsáveis pela infraestrutura crítica

[2] Consulte 15 U.S.C§272(e)(1)(A)(i). A Lei de Melhoria da Segurança Cibernética de 2014 (S.1353) The Cybersecurity Enhancement Act of 2014 (S.1353) tornou-se a lei pública n.o113-274 em 18 de dezembro de 2014 e pode ser acessada em: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Decreto n.º 13636, Aperfeiçoando a segurança cibernética da infraestrutura crítica, DCPD-201300091, 12 de fevereiro de 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014 -title3-vol1-eo13636.pdf

[4] O programa de infraestrutura crítica do Departamento de Segurança Interna (DHS) fornece uma lista dos setores e suas funções críticas e cadeias de valor relacionadas. http://www.dhs.gov/critical-infrastructure-sectors.

[5] Ver 42 U.S.C § 5195c(e)). A Lei Patriótica dos EUA de 2001 (H.R.3162) tornou-se direito público 107-56 em 26 de outubro de 2001 e pode ser encontrada em: https://www.congress.gov/bill/107th-congress/house-bill/3162.

precisam ter uma abordagem consistente e interativa para identificar, avaliar e gerenciar o risco de segurança cibernética. Essa abordagem é necessária, independentemente do tamanho de uma organização, exposição a ameaças ou nível atual de sofisticação de sua segurança cibernética.

A comunidade de infraestruturas críticas inclui proprietários, gestores públicos e privados, e outras entidades com a função de proteger a infraestrutura da nação. Os membros de cada setor de infraestrutura crítica têm funções que são apoiadas pela ampla categoria dos profissionais de tecnologia, incluindo a tecnologia da informação (TI), os sistemas de controle industrial (ICS, em inglês), os sistemas ciber-físicos (CPS, em inglês) e os dispositivos conectados de forma mais ampla, incluindo a Internet das Coisas (IoT, em inglês). Essa dependência de tecnologia, comunicação e interconectividade mudou e aprofundou as possíveis vulnerabilidades, e também aumentou o risco potencial para as operações. Por exemplo, à medida que a tecnologia, os dados que ela produz e os processos são cada vez mais utilizados para prestar serviços críticos e apoiar decisões empresariais ou a missão de determinada instituição, é fundamental analisar os possíveis impactos de um incidente de segurança cibernética em uma organização, na segurança e saúde dos indivíduos, no meio ambiente, em comunidades e na economia e na sociedade em geral.

Para gerenciar os riscos de segurança cibernética, faz-se necessário um entendimento claro dos indicadores de negócio da organização, além de considerações de segurança específicas a sua utilização da tecnologia. Como os riscos, as prioridades e os sistemas de cada organização são diferentes, haverá variações quanto às ferramentas e aos métodos utilizados para alcançar os resultados apresentados por este Guia.

Ao reconhecer o papel que a proteção de privacidade e das liberdades civis desempenha no desenvolvimento de uma confiança pública maior, o Guia inclui uma metodologia para proteger a privacidade individual e as liberdades civis quando as organizações de infraestrutura crítica realizam suas atividades que envolvem segurança cibernética. Muitas organizações já têm processos para lidar com a privacidade e as liberdades civis. A metodologia foi desenvolvida para complementar esses processos e fornecer orientações que facilitem o gerenciamento de riscos de privacidade de acordo com a abordagem de determinada organização no que tange ao gerenciamento de riscos de segurança cibernética.

A integração da privacidade e da segurança cibernética pode beneficiar as organizações ao aumentar a confiança do cliente, permitindo um compartilhamento de informações mais padronizado e simplificando as operações em todos os

sistemas jurídicos.

O Guia mantém-se efetivo e apoia a inovação técnica porque ele é tecnologicamente neutro, ao mesmo tempo em que faz referência a vários padrões, diretrizes e práticas existentes que se desenvolvem com a tecnologia. Baseando-se nesses padrões, diretrizes e práticas internacionais desenvolvidos, gerenciados e atualizados pela própria indústria, as ferramentas e os métodos disponíveis para alcançar os resultados do Guia irão ser ampliados para além das fronteiras, reconhecerão o caráter global dos riscos de segurança cibernética e evoluirão com os avanços tecnológicos e as demandas empresariais. O uso de padrões existentes e emergentes viabilizará as economias de escala e impulsionará o desenvolvimento de produtos, serviços e práticas eficazes que atendam às necessidades pertinentes a cada mercado. A competição de mercado também promove uma difusão mais rápida dessas tecnologias e práticas, assim como a realização de muitos benefícios pelos *stakeholders* desses setores.

Com base nesses padrões, diretrizes e práticas, o Guia oferece uma taxonomia e mecanismos comuns para que as organizações:

1) Descrevam sua situação atual no que tange à segurança cibernética;
2) Descrevam seus objetivos no que tange à segurança cibernética;
3) Identifiquem e priorizem oportunidades de aperfeiçoamento dentro do contexto de um processo contínuo e reproduzível;
4) Avaliem seus progressos frente aos objetivos:
5) Comuniquem-se com *stakeholders* internos e externos sobre os riscos apresentados na atual segurança cibernética.

Este Guia não se trata de uma abordagem única e exclusiva para gerenciar o risco de segurança cibernética em infraestruturas críticas. As organizações continuarão a ter seus próprios riscos — diferentes ameaças, vulnerabilidades, níveis de tolerâncias a riscos. Há variação também sobre como elas customizam as práticas descritas no Guia. As organizações podem determinar quais atividades são importantes para a entrega de serviços críticos e podem priorizar seus investimentos para aumentar o impacto de cada dólar investido.
Por fim, este Guia visa a reduzir e melhor gerenciar os riscos de segurança cibernética.

Para atender às necessidades específicas de segurança cibernética inerentes a cada organização, há uma grande variedade de maneiras de utilizar o Guia. A decisão sobre como aplicá-lo é responsabilidade da organização implementadora. Por

exemplo, uma organização pode optar por utilizar os Níveis de Implementação da Estrutura Básica para articular as práticas de gerenciamento de risco previstas. Uma outra organização pode usar as cinco funções da Estrutura Básica para analisar todo seu portfólio de gerenciamento de riscos. Essa análise pode ou não contar com orientações complementares mais detalhadas, como catálogos de controles. Às vezes há discussão sobre "*compliance*" com o Guia, sendo que o mesmo tem utilidade como uma estrutura e linguagem para organizar e apresentar o programa de *compliance* de acordo com os requisitos de segurança cibernética da própria organização. No entanto, a variedade de maneiras pelas quais o Guia pode ser usado por uma organização significa que frases como "*compliance* com o Guia" podem ser confusas e significar algo muito diferente para os vários *stakeholders* envolvidos no processo.

O Guia complementa e não substitui o processo de gerenciamento de segurança cibernética de uma organização ou seu programa de segurança cibernética em curso. A organização pode usar seus processos atuais e potencializá-los utilizando o Guia para identificar oportunidades que fortaleçam e comuniquem seu gerenciamento do risco de segurança cibernética, alinhando-se às práticas da indústria. Alternativamente, uma organização sem um programa de segurança cibernética pode usar o Guia como referência para implementar o seu.

Embora o Guia tenha sido desenvolvido para aperfeiçoar o gerenciamento do risco de segurança cibernética, uma vez que ele se relaciona com a infraestrutura crítica, ele pode ser utilizado por organizações em qualquer setor da economia ou da sociedade. Seu objetivo é ser útil para empresas, agências governamentais e organizações sem fins lucrativos, independentemente de sua área de atuação ou tamanho. A taxonomia comum de padrões, diretrizes e práticas que ele fornece também não é específica a nenhum país. As organizações fora dos Estados Unidos também podem usar o Guia para fortalecer seus próprios esforços de segurança cibernética. Além disso, o Guia pode contribuir para o desenvolvimento de uma linguagem comum para cooperação internacional em segurança cibernética da infraestrutura crítica.

1.1 Análise Geral do Guia

O Guia é uma abordagem baseada em riscos que visa auxiliar o gerenciamento do risco de segurança cibernética e é composto por três partes: a Estrutura Básica, os Níveis de Implementação e as Avaliações da Estrutura. Cada componente do Guia reforça a conexão entre os indicadores de negócio/missão e

as atividades de segurança cibernética. Esses componentes são explicados abaixo.

- A *Estrutura Básica* é um conjunto de atividades de segurança cibernética, resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica. A Estrutura Básica apresenta padrões, diretrizes e práticas da indústria de maneira a permitir a comunicação das atividades e dos resultados da segurança cibernética em toda a organização, desde o nível executivo até o nível de implementação ou operacional. A Estrutura Básica consiste de cinco funções simultâneas e contínuas — Identificar, Proteger, Detectar, Responder e Recuperar. Quando analisadas em conjunto, essas funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização. A Estrutura Básica identifica as principais Categorias e Subcategorias (as quais apresentam resultados discretos) para cada Função e as compara com exemplos de Referências Informativas, tais como padrões, diretrizes e práticas existentes para cada Subcategoria.
- *Os Níveis de Implementação da Estrutura* ("Níveis") apresentam contexto sobre como uma organização lida com o risco de segurança cibernética e os processos envolvidos para gerenciar esse risco. Os Níveis de Implementação descrevem o grau em que as práticas de gerenciamento do risco de segurança cibernética de determinada organização evidenciam as características definidas no Guia (por exemplo, consciência de risco e ameaça, reproduzível e adaptável). Os Níveis classificam as práticas de uma organização de Parcial (Nível 1) a Adaptável (Nível 4). Esses níveis refletem uma progressão de respostas informais e reativas a abordagens que são ágeis e baseadas no conhecimento dos riscos. Durante o processo de seleção de Nível, uma organização deve levar em consideração suas práticas atuais de gerenciamento de riscos, o ambiente de ameaças, requisitos legais e regulamentares, objetivos de negócio/missão, e suas restrições organizacionais.
- Uma Avaliação da Estrutura (“Avaliação”) representa os resultados com base nas necessidades empresariais que determinada organização selecionou a partir das Categorias e Subcategorias da Estrutura Básica. A Avaliação pode ser caracterizada como sendo a harmonização de padrões, diretrizes e práticas à Estrutura Básica em um cenário de implementação específico. As Avaliações podem ser usadas para identificar oportunidades de aprimoramento de sua situação no que tange à segurança cibernética, por

meio da comparação de uma Avaliação “atual” (o estado “como está”) com uma Avaliação “desejada” (o estado “a ser”). Para desenvolver uma Avaliação, uma organização pode avaliar todas as categorias e subcategorias e com base em seus indicadores de negócio/missão e uma avaliação de risco, determinar quais são as mais importantes. A organização pode adicionar Categorias e Subcategorias, conforme necessário, para enfrentar seus riscos. A Avaliação Atual pode então ser usada para dar apoio à priorização e à medição do progresso em direção à Avaliação Desejada, embora considere outras necessidades empresariais, incluindo a relação custo-benefício e a inovação. As Avaliações podem ser usadas para realizar autoavaliações e estabelecer comunicação dentro de uma organização ou entre organizações.

1.2 O Gerenciamento de Riscos e o Guia de Segurança Cibernética

O gerenciamento de riscos é o processo contínuo de identificação, avaliação e resposta ao risco. Para gerenciar riscos, as organizações devem entender a probabilidade de ocorrência de determinado evento e os possíveis impactos resultantes. Com essas informações, as organizações podem determinar o nível aceitável de risco para atingir seus objetivos organizacionais e podem, assim, apresentá-lo como sua tolerância a riscos.

Com uma compreensão da tolerância ao risco, as organizações podem priorizar as atividades de segurança cibernética, tornando-se capacitadas a tomar decisões sensatas quanto aos custos da segurança cibernética. A implementação de programas de gerenciamento de risco oferece às organizações a capacidade de quantificar e informar sobre ajustes em seus programas de segurança cibernética. As organizações podem optar por lidar com os riscos de maneiras diferentes, incluindo a mitigação do risco, a transferência do risco, a prevenção do risco ou a aceitação do risco, a depender de um eventual impacto na prestação de serviços críticos. O Guia utiliza processos de gerenciamento de riscos para permitir que as organizações informem e priorizem decisões relacionadas à segurança cibernética. Ele abrange avaliações de riscos recorrentes e a validação dos indicadores de negócio para ajudar as organizações a selecionar os níveis desejados de modo que as atividades de segurança cibernética reflitam os resultados desejados. Dessa forma, o Guia oferece às organizações a capacidade de selecionar e direcionar de forma dinâmica o aperfeiçoamento no gerenciamento de riscos de segurança cibernética para os ambientes de TI e ICS.

O Guia é adaptável para fornecer uma implementação flexível e baseada em conhecimento de riscos que possa ser usada com uma ampla gama de processos de gerenciamento de riscos de segurança cibernética. Exemplos de processos de gerenciamento de riscos de segurança cibernética incluem a Organização Internacional de Normalização (ISO, em inglês) 31000: 2009[6], ISO/Comissão Eletrotécnica Internacional (IEC, em inglês) 27005: 2011[7], Publicação Especial do NIST (SP) 800-39[8], e a orientação *Processo de Gerenciamento de Risco* (RMP) *de Segurança Cibernética do Subsetor de Eletricidade*[9].

1.3 Visão Geral do Documento

O restante deste documento contém as seguintes seções e anexos:

- A Seção 2 descreve os componentes do Guia: a Estrutura Básica, os Níveis e as Avaliações.
- A Seção 3 apresenta exemplos de como o Guia pode ser utilizado.
- A Seção 4 descreve como usar o Guia para autoavaliação e demonstração de segurança cibernética por meio de medições.
- O Anexo A apresenta a Estrutura Básica em um formato tabular: suas Funções, Categorias, Subcategorias e Referências Informativas.
- O Anexo B contém um glossário de termos selecionados.
- O Anexo C apresenta as siglas utilizadas neste documento.

[6] Organização Internacional de Normalização, Gerenciamento de riscos - Princípios e diretrizes, ISO 31000: 2009, 2009. http://www.iso.org/iso/home/standards/iso31000.html.
[7] Organização Internacional de Normalização /Comissão Eletrotécnica Internacional, Tecnologia da informação – Técnicas de segurança – Gerenciamento de riscos de segurança da informação, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html.
[8] Iniciativa Conjunta de Transformação do Grupo de Trabalho, Gerenciamento de Riscos de Segurança da Informação: Organization, Mission, and Information System View, Publicação Especial do NIST 800-39, março de 2011. https://doi.org/10.6028/NIST.SP.800-39.
[9] Departamento de Energia dos EUA, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003, maio de 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management ProcessGuideline-Final-May 2012.pdf

2.0 Noções Básicas do Guia

O Guia fornece uma linguagem comum para compreensão, gerenciamento e apresentação do risco de segurança cibernética para *stakeholders* internos e externos. Ele pode ser usado para ajudar a identificar e priorizar ações para reduzir o risco de segurança cibernética, e é uma ferramenta para harmonizar as abordagens de negócios, de políticas e de tecnologia para gerenciar esse risco. Ele pode ser usado para gerenciar os riscos de segurança cibernética em organizações inteiras ou pode ser focado na entrega de serviços críticos dentro de uma organização. Diferentes tipos de órgãos, incluindo estruturas de coordenação de setores, associações e organizações podem utilizar o Guia para fins diversos, incluindo a criação de Avaliações comuns.

2.1 Estrutura Básica

A Estrutura Básica fornece um conjunto de atividades para alcançar *resultados* específicos de segurança cibernética e faz referência a exemplos de diretrizes para que esses resultados sejam alcançados. A Estrutura Básica não é uma lista de verificação (*checklist*) de ações a serem executadas. Ela apresenta os principais resultados de segurança cibernética identificados pelos *stakeholders* e considerados úteis no gerenciamento do risco de segurança cibernética. A Estrutura Básica é composta por quatro elementos: Funções, Categorias, Subcategorias e Referências Informativas, conforme mostra a Imagem 1:

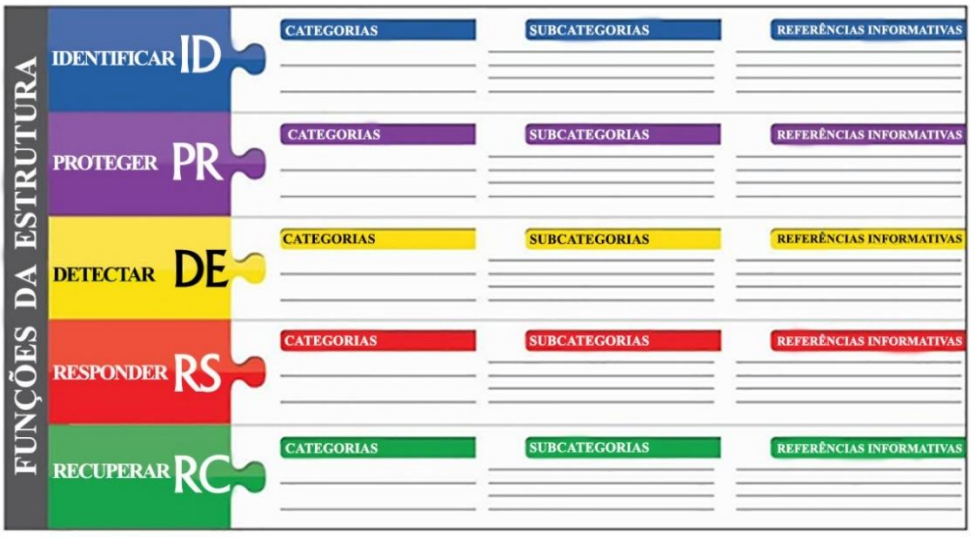

Figura 1: Organização da Estrutura Básica

Os elementos da Estrutura Básica funcionam juntos da seguinte forma:

- **Funções:** organizam atividades básicas de segurança cibernética em seu nível mais alto. Essas funções são: Identificar, Proteger, Detectar, Responder e Recuperar. Elas auxiliam uma organização a demonstrar seu gerenciamento de riscos de segurança cibernética, organizando as informações, possibilitando decisões de gerenciamento de riscos, tratando ameaças e aprimorando com base em atividades anteriores. As Funções também se alinham com as metodologias existentes para o gerenciamento de incidentes e ajudam a mostrar o impacto dos investimentos em segurança cibernética. Por exemplo, os investimentos em planejamento e treinamento compreendem ações de resposta e recuperação em tempo hábil, resultando em um impacto reduzido na entrega de serviços.
- **Categorias**: são as subdivisões de uma Função em grupos de resultados de segurança cibernética intimamente ligados a necessidades programáticas e atividades específicas. Exemplos de Categorias incluem "Gerenciamento de Ativos", "Gerenciamento de Identidades e Controle de Acesso" e "Processos de Detecção".
- **Subcategorias:** desmembram uma Categoria em resultados específicos de atividades técnicas e/ou de gerenciamento. Elas fornecem um conjunto de resultados que, embora não sejam exaustivos, ajudam a dar embasamento para a concretização dos resultados de cada Categoria. Alguns exemplos de subcategorias: "Catalogação de Sistemas de Informação Externos", "Proteção de Dados em Repouso" e "Investigação de Notificações de Sistemas de Detecção".
- **Referências Informativas:** são seções específicas sobre normas, diretrizes e práticas comuns entre os setores de infraestrutura crítica que ilustram um método para alcançar os resultados relacionados a cada subcategoria. As Referências Informativas apresentadas na Estrutura Básica são ilustrativas e exemplificativas. Elas são baseadas em orientações intersetoriais referenciadas com maior frequência durante o processo de desenvolvimento da Estrutura.

As cinco funções da Estrutura Básica são definidas abaixo. Essas funções não se destinam a formar um caminho sequencial ou levar a um estado final engessado. Em vez disso, as funções devem ser executadas simultânea e continuamente para criar uma cultura operacional que lide com o risco dinâmico da segurança cibernética. Veja o Anexo A para acesso à listagem completa da Estrutura Básica.

- **Identificar** - Desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos.

  As atividades na Função Identificar são fundamentais para o uso eficiente do Guia. Uma organização é capaz de focar e priorizar seus esforços de forma consistente com sua estratégia de gerenciamento de riscos e demandas empresariais, a partir da compreensão do contexto de seu nicho, dos recursos que suportam funções críticas e dos riscos de segurança cibernética envolvidos. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Ativos; Ambiente Empresarial; Governança; Avaliação de Risco; e Estratégia de Gerenciamento de Risco.

- **Proteger** - Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos.

  A Função Proteger fornece apoio à capacidade de limitar ou conter o impacto de uma possível ocorrência de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Gerenciamento de Identidade e Controle de Acesso; Conscientização e Treinamento; Segurança de dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção.

- **Detectar** - Desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética.

  A Função Detectar permite a descoberta oportuna de ocorrências de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Anomalias e Ocorrências; Monitoramento Contínuo de Segurança; e Processos de Detecção.

- **Responder** - Desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado.

  A Função Responder suporta a capacidade de conter o impacto de um possível incidente de segurança cibernética. Exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Resposta; Notificações; Análise; Mitigação; e Aperfeiçoamentos.

- **Recuperar** - Desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

  A Função Recuperar oferece apoio ao restabelecimento pontual para as

operações normais de modo a reduzir o impacto de determinado incidente de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Restabelecimento; Aperfeiçoamentos; e Notificações.

2.2 Níveis de Implementação da Estrutura

Os Níveis de Implementação da Estrutura ("Níveis") fornecem contexto sobre como determinada organização trata o risco de segurança cibernética e os processos envolvidos para gerenciamento desse risco. Variando de Parcial (Nível 1) a Nível Adaptável (Nível 4), os níveis descrevem um grau crescente de rigor e sofisticação nas práticas de gerenciamento de riscos de segurança cibernética. Os Níveis ajudam a determinar até que ponto o gerenciamento do risco de segurança cibernética é permeado pelas demandas empresariais e é integrado às práticas gerais de gerenciamento de risco de uma organização. As análises sobre gerenciamento de riscos contemplam muitos aspectos da segurança cibernética, incluindo o grau em que as considerações sobre privacidade e liberdades civis são integradas ao gerenciamento de risco de segurança cibernética e às possíveis respostas a riscos por parte de uma organização.

O processo de seleção de Nível considera as práticas atuais de gerenciamento de risco de uma organização, ambiente de ameaças, requisitos legais e regulamentares, práticas de compartilhamento de informações, objetivos de negócio/missão, requisitos de segurança cibernética da cadeia de suprimento e restrições organizacionais. As organizações devem determinar o Nível desejado, garantindo que o nível selecionado atenda às metas organizacionais, seja viável em sua implementação e reduza o risco de segurança cibernética em ativos e recursos críticos para níveis aceitáveis para a organização. As organizações devem considerar a possibilidade de potencializar a orientação externa obtida a partir de departamentos e agências do governo federal, Centros de Análise e Compartilhamento de Informação (ISACs, em inglês), Organizações de Análise e Compartilhamento de Informações (ISAOs, em inglês), modelos de maturidade existentes ou outras fontes para auxiliar na determinação do nível desejado.

Embora as organizações identificadas como Nível 1 (Parcial) sejam incentivadas a considerar a mudança para o nível 2 ou superior, os níveis não representam níveis de maturidade. Os níveis destinam-se a apoiar a tomada de decisão organizacional sobre como gerenciar o risco de segurança cibernética, bem como quais dimensões da organização têm maior prioridade e podem receber recursos adicionais. A

progressão para níveis mais altos é incentivada quando uma análise de custo-benefício indica uma redução viável e econômica do risco de segurança cibernética.

A implementação bem-sucedida ao Guia é mensurada a partir da obtenção dos resultados descritos na(s) Avaliação(Avaliações) Desejada(s) da organização e não na determinação do Nível. Ainda assim, a seleção e a designação do Nível normalmente afetam as Avaliações da Estrutura. A recomendação de Nível por parte de gerentes de negócio e de nível de processo, e aprovada pelo Administrador, ajudará a definir a linha geral de como o risco de segurança cibernética será gerenciado dentro da organização e deve influenciar a priorização dentro de uma *Avaliação Desejada* e as avaliações de progresso na tratativa das lacunas.

As definições de Níveis são as seguintes:

Nível 1: Parcial

- *Processo de Gerenciamento de Risco* - As práticas de gerenciamento de risco de segurança cibernética organizacional não são formalizadas, e o risco é gerenciado de maneira *ad hoc* e às vezes reativa. A priorização das atividades de segurança cibernética pode não estar diretamente permeada pelos objetivos de risco organizacionais, pelo ambiente de ameaças ou pelos requisitos de negócios/missão.
- *Programa Integrado de Gerenciamento de Risco* - Existe uma consciência limitada do risco de segurança cibernética no nível organizacional. A organização implementa o gerenciamento de riscos de segurança cibernética de maneira irregular, caso a caso, devido à experiência variada ou a informações obtidas de fontes externas. A organização pode não ter processos que permitam que as informações de segurança cibernética sejam compartilhadas internamente.
- *Participação Externa* - A organização não entende seu papel no ecossistema maior com relação a suas dependências ou dependentes. A organização não colabora com ou recebe informações (por exemplo, inteligência de ameaças, melhores práticas, tecnologias) de outras entidades (por exemplo, compradores, fornecedores, dependências, dependentes, ISAOs, pesquisadores, governos), nem compartilha informações. A organização geralmente não tem consciência dos riscos da cadeia de suprimentos cibernéticos dos produtos e serviços que fornece e que usa.

Nível 2: Risco Informado

- *Processo de Gerenciamento de Risco* - As práticas de gerenciamento de risco são aprovadas pela administração, mas podem não ser estabelecidas como políticas para toda a organização. A priorização das atividades de segurança cibernética e as necessidades de proteção são permeadas diretamente pelos objetivos de risco organizacionais, pelo ambiente de ameaças ou pelos requisitos de negócios/missão.
- *Programa Integrado de Gerenciamento de Risco* - Há uma conscientização do risco de segurança cibernética no nível organizacional, mas não foi estabelecida uma abordagem válida para toda a organização para gerenciar o risco de segurança cibernética. Informações de segurança cibernética são compartilhadas informalmente dentro da organização. Atenção à segurança cibernética em objetivos e programas organizacionais pode ocorrer em alguns, mas não em todos os níveis da organização. A avaliação do risco cibernético de ativos organizacionais e externos ocorre, mas não é tipicamente reproduzível ou recorrente.
- *Participação Externa* - Geralmente, a organização entende seu papel no ecossistema maior com relação as suas próprias dependências ou dependentes, mas não a ambos. A organização colabora e recebe algumas informações de outras entidades e gera algumas de suas próprias informações, mas pode não compartilhar informações com outras pessoas. Além disso, a organização está ciente dos riscos da cadeia de suprimentos cibernéticos associados aos produtos e serviços que fornece e usa, mas não age de maneira consistente ou formal sobre esses riscos.

Nível 3: Reproduzível

- *Processo de Gerenciamento de Risco* - As práticas de gerenciamento de risco da organização são formalmente aprovadas e expressas como política. Práticas organizacionais de segurança cibernética são atualizadas regularmente com base na aplicação dos processos de gerenciamento de riscos às mudanças nos requisitos de negócios/missão em cenário dinâmico de ameaças e tecnologia.
- *Programa Integrado de Gerenciamento de Risco* - Existe uma abordagem para toda a organização para gerenciar o risco de segurança cibernética. Políticas, processos e procedimentos de conhecimento de riscos são definidos, implementados conforme pretendido e revisados. Existem métodos consistentes para responder de forma eficaz às mudanças no risco. Os funcionários possuem

o conhecimento e as habilidades para desempenhar suas funções e responsabilidades. A organização monitora consistentemente e com precisão o risco de segurança cibernética dos ativos organizacionais. Executivos seniores de segurança cibernética e executivos de outras áreas se comunicam regularmente sobre o risco de segurança cibernética. Executivos seniores asseguram a análise da segurança cibernética em todas as linhas de operação da organização.

- *Participação Externa* - A organização entende seu papel, dependências e dependentes no ecossistema maior e pode contribuir para o entendimento mais amplo da comunidade sobre os riscos. Colabora e recebe regularmente informações de outras entidades que complementam informações geradas internamente, e compartilha informações com outras entidades. A organização está ciente dos riscos da cadeia de suprimentos cibernéticos associados aos produtos e serviços que ela fornece e que ela utiliza. Além disso, geralmente age formalmente sobre esses riscos, incluindo mecanismos como acordos por escrito para comunicar requisitos básicos, estruturas de governança (por exemplo, conselhos de riscos) e implantação e monitoramento de políticas.

Nível 4: Adaptável

- *Processo de Gerenciamento de Risco* - A organização adapta suas práticas de segurança cibernética com base em atividades de segurança cibernética anteriores e atuais, incluindo lições aprendidas e indicadores preditivos. Por meio de um processo de aperfeiçoamento contínuo que incorpora tecnologias e práticas avançadas de segurança cibernética, a organização se adapta ativamente a um cenário de ameaças e tecnologias em constante mudança e responde de maneira oportuna e eficaz às ameaças sofisticadas e em evolução.
- *Programa Integrado de Gerenciamento de Risco* - Existe uma abordagem para toda a organização para o gerenciamento do risco de segurança cibernética que usa políticas, processos e procedimentos de conhecimento de risco para tratar possíveis ocorrências de segurança cibernética. A relação entre o risco de segurança cibernética e os objetivos organizacionais é claramente entendida e analisada durante o processo de tomada de decisões. Executivos seniores monitoram o risco de segurança cibernética no mesmo contexto que o risco financeiro e outros riscos organizacionais. O orçamento organizacional baseia-se na compreensão do ambiente de risco atual e o previsto, assim como na compreensão da tolerância ao risco. As unidades de negócios implementam a visão executiva e analisam os riscos no nível do sistema no contexto das

tolerâncias de risco organizacionais. O gerenciamento de riscos de segurança cibernética faz parte da cultura organizacional e evolui a partir da conscientização das atividades anteriores e da conscientização contínua das atividades em seus sistemas e redes. A organização pode responder de forma rápida e eficiente às mudanças nos objetivos de negócio/missão sobre como o risco é abordado e comunicado.

- *Participação Externa* - A organização entende seu papel, dependências e dependentes no ecossistema maior e contribui para a compreensão mais ampla da comunidade sobre os riscos. Ela recebe, gera e analisa informações priorizadas que informam a análise contínua de seus riscos à medida que os cenários de ameaças e tecnologia evoluem. A organização compartilha essas informações internamente e externamente com outros colaboradores. A organização usa informações em tempo real ou quase em tempo real para entender e agir de forma consistente sobre os riscos da cadeia de suprimentos cibernéticos associados aos produtos e serviços que ela oferece e utiliza. Além disso, a organização se comunica de forma proativa, usando mecanismos formais (por exemplo, acordos) e informais para desenvolver e manter fortes relacionamentos com a cadeia de fornecimento.

2.3 Avaliação da Estrutura

A Avaliação da Estrutura ("Avaliação") é o alinhamento das Funções, Categorias e Subcategorias com os requisitos de negócios, a tolerância a riscos e os recursos da organização. Uma Avaliação permite que as organizações estabeleçam um roteiro para reduzir o risco de segurança cibernética que esteja bem alinhado com as metas organizacionais e setoriais, considere os requisitos legais/regulatórios e as melhores práticas do setor e reflita as prioridades de gerenciamento de riscos. Dada a complexidade de muitas organizações, elas podem optar por ter várias avaliações, alinhadas a componentes específicos e reconhecendo suas necessidades individuais.

As Avaliações de Estrutura podem ser usadas para descrever o estado atual ou o estado desejado de atividades específicas de segurança cibernética. A Avaliação Atual indica os resultados da segurança cibernética que estão sendo alcançados atualmente. A Avaliação Desejada indica os resultados necessários para atingir as metas desejadas de gerenciamento de riscos de segurança cibernética. As avaliações suportam os requisitos de negócios/missão e auxiliam na comunicação de riscos dentro e entre organizações. Este quadro não prescreve modelos de

Avaliações, permitindo flexibilidade na implementação.

A comparação de avaliações (por exemplo, a Avaliação Atual e a Avaliação Desejada) pode revelar as lacunas a serem tratadas de modo a atender aos objetivos de gerenciamento de riscos da segurança cibernética. Um plano de ação para resolver essas lacunas para satisfazer a uma determinada Categoria ou Subcategoria pode contribuir para o roteiro descrito acima. A priorização da mitigação de lacunas é impulsionada pelas necessidades de negócios da organização e pelos processos de gerenciamento de riscos. Essa abordagem baseada em risco permite que uma organização avalie os recursos necessários (por exemplo, funcionários, financeiro) para atingir as metas de segurança cibernética de maneira econômica e priorizada. Além disso, o Guia é uma abordagem de conhecimento de risco, em que a aplicabilidade e o desempenho de determinada Subcategoria estão sujeitos ao alcance da Avaliação.

2.4 Coordenação da Implementação do Guia

A Figura 2 descreve um fluxo comum de informações e decisões nos seguintes níveis dentro de uma organização:

- Executivo
- Negócio/Processo
- Implementação/Operações

O nível executivo transmite as prioridades da missão, os recursos disponíveis e tolerância geral ao risco para o nível de negócio/processo. O nível de negócio/processo usa as informações como contribuições no processo de gerenciamento de riscos e colabora com o nível de implementação/operações para comunicar as necessidades de negócios e criar uma Avaliação. O nível de implementação/operações transmite o progresso da implementação da Avaliação ao nível de negócio/processo. O nível de negócio/processo usa essas informações para realizar uma avaliação de impacto. O gerenciamento de nível de negócio/processo reporta os resultados dessa avaliação de impacto ao nível executivo para informar o processo geral de gerenciamento de risco da organização para o nível de implementação/operações e conscientização do impacto nos negócios.

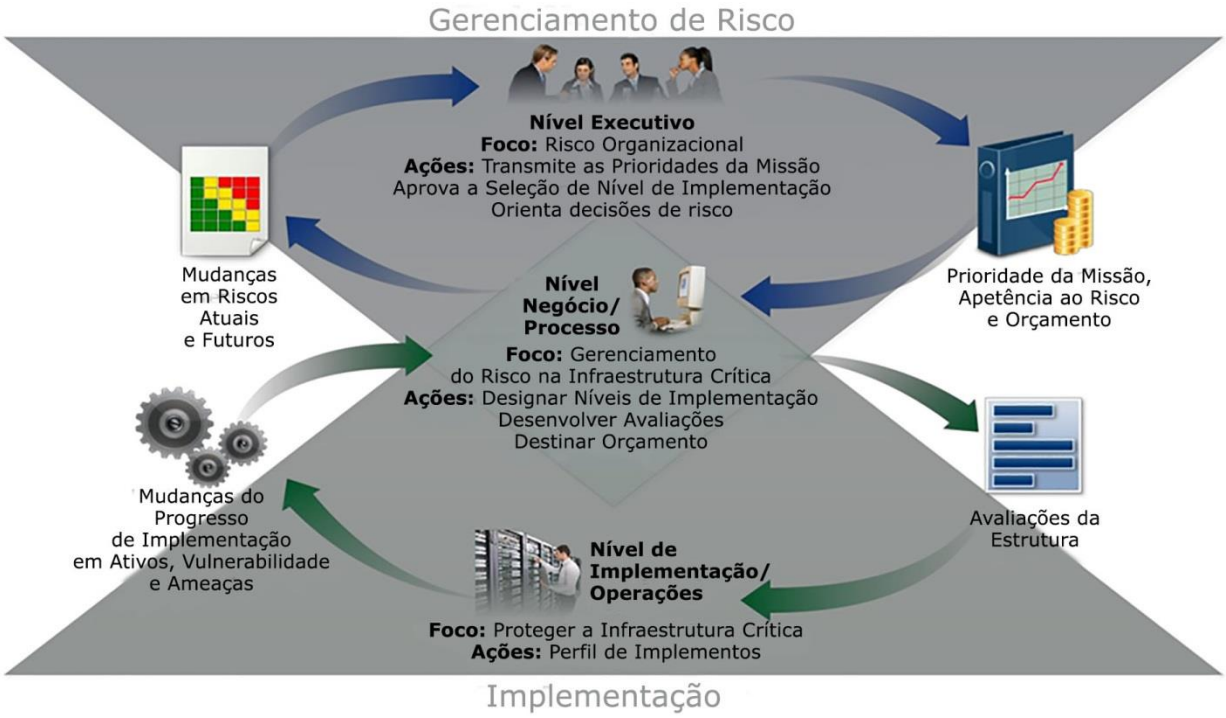

Figura 2: Informações Teóricas e Fluxos de Decisão dentro de uma Organização

3.0 Como Utilizar o Guia

Uma organização pode usar o Guia como parte fundamental de seu processo sistemático para identificar, avaliar e gerenciar o risco de segurança cibernética. O Guia não foi projetado para substituir os processos existentes; uma organização pode usar seu processo atual e sobrepô-lo ao Guia para determinar lacunas em sua atual abordagem de risco de segurança cibernética e desenvolver um roteiro para aperfeiçoamento. Usando o Guia como uma ferramenta de gerenciamento de risco de segurança cibernética, uma organização pode determinar as atividades que são mais importantes para a entrega de serviços críticos e priorizar as despesas para maximizar o impacto do investimento.

O Guia é projetado para complementar as operações existentes de negócios e segurança cibernética. Ele pode servir como base para um novo programa de segurança cibernética ou um mecanismo para melhorar um programa existente. O Guia fornece um meio de expressar os requisitos de segurança cibernética para parceiros de negócios e clientes e pode ajudar a identificar falhas nas práticas de segurança cibernética de uma organização. Ele também fornece um conjunto geral de processos e ponderações para considerar as implicações de privacidade e as liberdades civis no contexto de um programa de segurança cibernética.

O Guia pode ser aplicado em todas as fases do ciclo de vida do plano, *design*, desenvolvimento/compra, implantação, operação e desativação. A fase de planejamento inicia o ciclo de qualquer sistema e estabelece as bases para tudo o que se segue. Considerações gerais sobre segurança cibernética devem ser anunciadas e descritas da forma mais clara possível. O plano deve reconhecer que essas considerações e requisitos provavelmente evoluirão durante o restante do ciclo de vida. A fase de design deve considerar os requisitos de segurança cibernética como parte de um processo multidisciplinar maior de engenharia de sistemas[10]. Um marco importante da fase de projeto é a validação de que as especificações de segurança cibernética do sistema correspondem às necessidades e à disposição da organização, como identificado na Avaliação da Estrutura. Os resultados desejados de segurança cibernética, priorizados em uma Avaliação Desejada, devem ser incorporados quando a) desenvolver o sistema durante a fase de construção e b) comprar ou terceirizar o sistema durante a fase de compra. Essa mesma Avaliação

[10] NIST Publicação Especial 800-160 Volume 1, Engenharia de Segurança do Sistema, Considerações para uma Abordagem Multidisciplinar na Engenharia de Sistemas Seguros e Confiáveis, Ross et al, novembro de 2016 (atualizado em 21 de março de 2018), https: //doi.org/10.6028/NIST.SP.800-160v1

Desejada serve como uma lista de recursos de segurança cibernética do sistema, que devem ser avaliados durante a implantação do sistema para verificar se todos os recursos estão implementados. Os resultados da segurança cibernética determinados pelo uso do Guia devem servir como base para a operação contínua do sistema. Isso inclui reavaliações ocasionais, registrando os resultados em uma Avaliação Atual, para verificar se os requisitos de segurança cibernética ainda estão sendo atendidos. Tipicamente, uma teia complexa de dependências (por exemplo, controles comuns e compensatórios) entre sistemas significa que os resultados documentados em Avaliações Desejadas de sistemas relacionados devem ser cuidadosamente considerados à medida que os sistemas são desativados.

As seções a seguir apresentam diferentes maneiras em que as organizações podem usar o Guia.

3.1 Avaliação Básica das Práticas de Segurança Cibernética

O Guia pode ser usado para comparar as atividades de segurança cibernética atuais de uma organização com as descritas na Estrutura Básica. Por meio da criação de uma Avaliação Atual, as organizações podem examinar até que ponto estão atingindo os resultados descritos nas Categorias Principais e nas Subcategorias, alinhadas com as cinco Funções de alto nível: Identificar, Proteger, Detectar, Responder e Recuperar. Uma organização pode achar que já está atingindo os resultados desejados, gerenciando, assim, a segurança cibernética proporcional ao risco conhecido. Alternativamente, uma organização pode determinar que tem oportunidades para (ou que precisa) aperfeiçoar. A organização pode usar essas informações para desenvolver um plano de ação para fortalecer as práticas existentes e reduzir o risco de segurança cibernética. Uma organização também pode descobrir que está investindo demais para alcançar certos resultados. A organização pode usar essas informações para reavaliar a priorização de recursos.

Embora não substituam um processo de gerenciamento de riscos, essas cinco funções de alto nível fornecerão uma maneira concisa para executivos seniores e outros filtrarem os conceitos fundamentais de risco de segurança cibernética, de modo que possam avaliar como os riscos identificados são gerenciados e como suas organizações se portam em um alto nível frente aos padrões, diretrizes e práticas existentes de segurança cibernética. O Guia também pode ajudar uma organização a responder perguntas fundamentais, incluindo "Como estamos?" Então, podem se movimentar de maneira mais informada para fortalecer suas práticas de segurança cibernética onde e quando julgarem necessário.

3.2 Elaboração ou Melhoria de um Programa de Segurança Cibernética

As etapas abaixo ilustram como uma organização pode usar o Guia para criar um novo programa de segurança cibernética ou aperfeiçoar um programa existente. Estas etapas devem ser repetidas conforme necessário para um aperfeiçoamento contínuo da segurança cibernética.

Etapa 1: Priorize e determine o Escopo. A organização identifica seus objetivos de negócios/missão e prioridades organizacionais de alto nível. Com essas informações, a organização toma decisões estratégicas sobre implementações de segurança cibernética e determina o escopo de sistemas e ativos que suportam a linha de negócios ou processo selecionado. O Guia pode ser adaptado para suportar as diferentes linhas de negócios ou processos dentro de uma organização, que podem ter diferentes necessidades empresariais e tolerância a riscos associados. As tolerâncias a riscos podem ser refletidas em um Nível de Implementação desejado.

Etapa 2: Oriente. Uma vez que o escopo do programa de segurança cibernética tenha sido determinado para a linha de negócios ou processo, a organização identifica sistemas e ativos relacionados, os requisitos regulatórios e a abordagem geral de risco. A organização então consulta fontes para identificar ameaças e vulnerabilidades aplicáveis aos sistemas e ativos.

Etapa 3: Crie uma Avaliação Atual. A organização desenvolve uma Avaliação Atual, indicando quais resultados de Categoria e Subcategoria da Estrutura Básica estão sendo alcançados no momento. Se um resultado for parcialmente alcançado, observar esse fato ajudará a dar suporte às etapas subsequentes, fornecendo informações básicas.

Etapa 4: Realize uma avaliação de risco. Esta avaliação pode ser guiada pelo processo geral de gerenciamento de riscos da organização ou atividades anteriores de avaliação de risco. A organização analisa o ambiente operacional para identificar a probabilidade de uma ocorrência de segurança cibernética e o impacto que tal ocorrência poderia ter na organização. É importante que as organizações identifiquem os riscos emergentes e usem informações de ameaças cibernéticas de fontes internas e externas para obter uma melhor compreensão da probabilidade e do impacto de ocorrências de segurança cibernética.

Etapa 5: Criar uma Avaliação Desejada. A organização cria uma Avaliação Desejada que enfoca a avaliação das Categorias e Subcategorias do Guia, descrevendo os resultados de segurança cibernética desejados pela organização. As organizações também podem desenvolver suas próprias Categorias adicionais e Subcategorias para atender a riscos organizacionais singulares. A organização também pode considerar influências e requisitos dos *stakeholders* externos, tais como entidades do setor, clientes e parceiros de negócios ao criar uma Avaliação Desejada. A Avaliação Desejada deve refletir os critérios adequadamente dentro do Nível de Implementação desejado.

Etapa 6: Determinar, Analisar e Priorizar as Falhas. A organização compara a Avaliação Atual e a Avaliação Desejada para determinar as lacunas. Em seguida, ela cria um plano de ação priorizado para consertar as lacunas — refletindo os indicadores da missão, custos e benefícios e riscos — para alcançar os resultados na Avaliação Desejada. A organização então define os recursos necessários, incluindo financeiros e laborais para tratar as lacunas. O uso das Avaliações dessa maneira incentiva a organização a tomar decisões fundamentadas sobre as atividades de segurança cibernética, oferece suporte ao gerenciamento de riscos e permite que a organização realize aperfeiçoamentos direcionados com boa relação custo-benefício.

Etapa 7: Implementar o Plano de Ação. A organização determina quais ações devem ser tomadas para tratar as lacunas, se houver, identificadas na etapa anterior e, em seguida, ajusta suas práticas atuais de segurança cibernética para alcançar a Avaliação Desejada. Para orientação adicional, o Guia identifica exemplos de Referências Informativas referentes às Categorias e Subcategorias, sendo que as organizações devem determinar quais padrões, diretrizes e práticas, incluindo aquelas que são específicas de seu setor, funcionam melhor para suas necessidades.

Uma organização repete as etapas conforme necessário para avaliar e aperfeiçoar continuamente sua segurança cibernética. Por exemplo, as organizações podem descobrir que a repetição mais frequente da etapa "Oriente" (Etapa 2) aperfeiçoa a qualidade das avaliações de risco. Além disso, as organizações podem monitorar o progresso por meio de atualizações iterativas na Avaliação Atual, comparando posteriormente a Avaliação Atual à Avaliação Desejada. As organizações também podem usar esse processo para alinhar seu programa de segurança cibernética com o Nível de Implementação de Estrutura desejado.

3.3 Informar os *stakeholders* sobre os Requisitos de Segurança Cibernética

O Guia fornece uma linguagem comum para informar os requisitos entre os *stakeholders* interdependentes responsáveis pela entrega de produtos e serviços essenciais de infraestrutura crítica. Os exemplos incluem:

- Uma organização pode usar uma Avaliação Desejada para expressar os requisitos de gerenciamento de risco de segurança cibernética a um provedor de serviços externo (por exemplo, um provedor de armazenamento em nuvem para o qual ele está exportando dados).
- Uma organização pode expressar seu estado de segurança cibernética por meio de uma Avaliação Atual para relatar resultados ou para compará-los com os requisitos de aquisição.
- Um proprietário/operador de infraestrutura crítica, tendo identificado um parceiro externo de quem depende essa infraestrutura, pode usar uma Avaliação Desejada para entregar as Categorias e Subcategorias necessárias.
- Um setor de infraestrutura crítica pode estabelecer uma Avaliação Desejada que possa ser usada entre seus constituintes como uma avaliação básica inicial para desenvolver suas Avaliações Desejadas sob medida.
- Uma organização pode gerenciar melhor o risco de segurança cibernética entre os *stakeholders*, avaliando sua posição na infraestrutura crítica e na economia digital mais ampla usando os níveis de implementação.

A comunicação é especialmente importante entre os *stakeholders* nos níveis superiores e inferiores nas cadeias de suprimentos. As cadeias de suprimentos são complexas, distribuídas globalmente e também são grupos interconectados de recursos e processos entre os vários níveis de organizações. As cadeias de suprimento têm início no provimento de produtos e serviços e se estendem até o projeto, desenvolvimento, fabricação, processamento, manuseio e entrega de produtos e serviços até o usuário final. Dadas essas relações complexas e interconectadas, o Gerenciamento de Riscos em Cadeias de Suprimentos (SCRM, em inglês) é uma função organizacional crítica[11].

O SCRM cibernético é o conjunto de atividades necessárias para gerenciar os riscos de segurança cibernética associados a partes externas. Mais especificamente, o SCRM cibernético trata o efeito de segurança cibernética que

[11] Informar sobre os Requisitos de Segurança Cibernética (Seção 3.3) e as Decisões de Compra (Seção 3.4) abordam apenas dois usos do Guia para o SCRM cibernético e não se destinam a abordar o SCRM cibernético de forma abrangente.

uma organização tem em partes externas e o efeito de segurança cibernética que as partes externas têm em uma organização.

Um objetivo primário do SCRM cibernético é identificar, avaliar e mitigar “produtos e serviços que possam conter funcionalidade potencialmente maliciosa, sejam falsificados ou vulneráveis devido a práticas inadequadas de fabricação e desenvolvimento dentro da cadeia de suprimentos cibernéticos[12]." As atividades de SCRM cibernético podem incluir:

- Determinar os requisitos de segurança cibernética para fornecedores,
- Aprovar/promulgar requisitos de segurança cibernética através de acordo formal (por exemplo, contratos),
- Comunicar aos fornecedores como os requisitos de segurança cibernética serão verificados e validados,
- Verificar se os requisitos de segurança cibernética são atendidos através de uma variedade de metodologias de avaliação, e
- Regular/administrar e gerenciar as atividades listadas acima.

Como mostrado na Figura 3, o SCRM cibernético abrange fornecedores e compradores de tecnologia, bem como fornecedores e compradores de outras áreas, onde a tecnologia é minimamente composta de tecnologia da informação (TI), sistemas de controle industrial (ICS), sistemas ciber-físicos (CPS) e dispositivos conectados de forma mais geral, incluindo a Internet das Coisas (IoT). A Figura 3 mostra uma organização em um único ponto no tempo. Entretanto, durante o curso normal das operações comerciais, a maioria das organizações será tanto um fornecedor a montante e um comprador a jusante em relação a outras organizações ou usuários finais.

[12] NIST Publicação Especial 800-161, Práticas de Gerenciamento de riscos em cadeias de suprimentos para Organizações e Sistemas Governamentais, Boyens et al, abril de 2015, https://doi.org/10.6028/NIST.SP.800-161

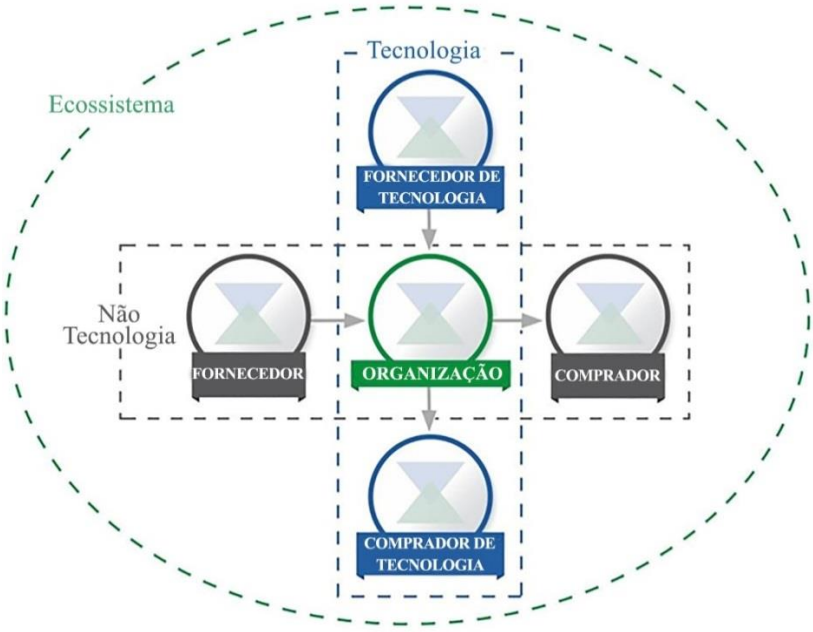

Figura 3: Relacionamentos da Cadeia de Suprimentos Cibernéticos

As partes descritas na Figura 3 compõem o ecossistema de segurança cibernética de uma organização. Esses relacionamentos destacam o papel crucial do SCRM Cibernético no tratamento ao risco de segurança cibernética na infraestrutura crítica e na economia digital mais ampla. Esses relacionamentos, os produtos e serviços que eles fornecem e os riscos que eles apresentam devem ser identificados e incluídos nas capacidades de proteção e detecção das organizações, assim como seus protocolos de resposta e recuperação.

Na imagem acima, o termo "Comprador" refere-se às pessoas ou organizações a jusante que consomem um determinado produto ou serviço de uma organização, incluindo organizações com e sem fins lucrativos. O termo "Fornecedor" abrange fornecedores de produtos e serviços a montante, que são usados para fins internos de uma organização (por exemplo, infraestrutura de TI) ou integrados aos produtos ou serviços fornecidos ao Comprador. Estes termos são aplicáveis a produtos e serviços baseados em tecnologia e não baseados em tecnologia.

Seja considerando Subcategorias individuais da Estrutura Básica ou as considerações abrangentes de uma Avaliação, o Guia oferece às organizações e seus parceiros um método para ajudar a garantir que o novo produto ou serviço atenda a resultados críticos de segurança. Ao selecionar primeiro os resultados que

são relevantes para o contexto (por exemplo, transmissão de informações pessoalmente identificáveis (PII), prestação de serviços críticos da missão, serviços de verificação de dados, integridade de produtos ou serviços), a organização pode então avaliar seus parceiros em relação a esses critérios. Por exemplo, se um sistema está sendo comprado que monitora a Tecnologia Operacional (OT) para comunicação de rede anômala, a disponibilidade pode ser um objetivo de segurança cibernética particularmente importante a ser alcançado e deve nortear uma avaliação de Fornecedor de Tecnologia em relação às Subcategorias aplicáveis (por exemplo, ID. SER-4, ID. SC-3, ID. SC-4, ID. SC-5, PR. DS-4, PR. DS-6, PR. DS-7, PR. DS-8, PR. IP-1, DE. AE-5).

3.4 Decisões de Compra

Como uma Avaliação Desejada da Estrutura é uma lista priorizada de requisitos organizacionais de segurança cibernética, as Avaliações Desejadas podem ser usadas para basear decisões de compra de produtos e serviços. Essa transação varia desde Informar os *Stakeholders* sobre os Requisitos de Segurança Cibernética (abordado na Seção 3.3), pois pode não ser possível impor um conjunto de requisitos de segurança cibernética ao fornecedor. O objetivo deve ser tomar a melhor decisão de compra dentre vários fornecedores, tendo em vista uma lista cuidadosamente determinada de requisitos de segurança cibernética. Muitas vezes, isso significa algum grau de compensação (*trade-off*), comparando vários produtos ou serviços com as lacunas conhecidas para a Avaliação Desejada.

Quando um produto ou serviço é adquirido, a Avaliação também pode ser usada para rastrear e tratar o risco residual de segurança cibernética. Por exemplo, se o serviço ou produto comprado não atender a todos os objetivos descritos na Avaliação Desejada, a organização pode tratar o risco residual por meio de outras ações de gerenciamento. A Avaliação também fornece à organização um método para avaliar se o produto atende aos resultados de segurança cibernética por meio de mecanismos periódicos de análise e teste.

3.5 Identificando Oportunidades para Referências Informativas Novas ou Revisadas

O Guia pode ser usado para identificar oportunidades de padrões, diretrizes ou

práticas novas ou revisadas, nas quais as Referências Informativas adicionais podem ajudar as organizações a tratar as demandas emergentes. Ao implementar uma determinada subcategoria, ou desenvolvendo uma nova subcategoria, uma organização pode descobrir que existem poucas, ou nenhuma, Referências Informativas para uma atividade relacionada. Para atender a essa necessidade, a organização pode colaborar com líderes de tecnologia e/ou órgãos de normas para redigir, desenvolver e coordenar padrões, diretrizes ou práticas.

3.6 Metodologia para Proteger a Privacidade e as Liberdades Civis

Esta seção descreve uma metodologia para tratar as implicações individuais de privacidade e liberdades civis que podem resultar da segurança cibernética. Esta metodologia tem como principal objetivo ser um conjunto geral de considerações e processos, uma vez que as implicações de privacidade e liberdades civis podem diferir entre os setores ou ao longo do tempo, e as organizações podem abordar essas considerações e processos com uma série de implementações técnicas. No entanto, nem todas as atividades em um programa de segurança cibernética geram considerações sobre privacidade e liberdades civis. Padrões técnicos de privacidade, diretrizes e melhores práticas adicionais podem precisar ser desenvolvidos para suportar implementações técnicas aperfeiçoadas.

A Privacidade e a segurança cibernética têm uma conexão muito forte. As atividades de segurança cibernética de uma organização também podem criar riscos à privacidade e às liberdades civis quando informações pessoais são usadas, coletadas, processadas, mantidas ou divulgadas. Alguns exemplos incluem: atividades de segurança cibernética que resultam na coleta excessiva ou na retenção excessiva de informações pessoais; divulgação ou uso de informações pessoais não relacionadas às atividades de segurança cibernética; e atividades de mitigação de segurança cibernética que resultam em negação de serviço ou outros impactos potencialmente adversos semelhantes, incluindo alguns tipos de detecção ou monitoramento de incidentes que podem inibir a liberdade de expressão ou associação.

O governo e seus agentes têm a responsabilidade de proteger as liberdades civis decorrentes das atividades de segurança cibernética. Conforme mencionado na metodologia abaixo, o governo ou seus agentes que possuem ou operam infraestrutura crítica devem ter um processo em vigor para apoiar *compliance* das

atividades de segurança cibernética com as leis de privacidade, regulamentos e requisitos constitucionais aplicáveis.

Para lidar com as implicações de privacidade, as organizações podem considerar como seus programas de segurança cibernética podem incorporar princípios de privacidade, tais como: minimização de dados na coleta, divulgação e retenção de material de informações pessoais relacionadas ao incidente de segurança cibernética; uso de limitações fora das atividades de segurança cibernética em qualquer informação coletada especificamente para atividades de segurança cibernética; transparência para certas atividades de segurança cibernética; consentimento individual e reparação de impactos adversos decorrentes do uso de informações pessoais em atividades de segurança cibernética; qualidade, integridade e segurança dos dados; e prestação de contas e auditoria.

Como as organizações avaliam a Estrutura Básica no Anexo A, os seguintes processos e atividades podem ser considerados como um meio de lidar com as implicações de privacidade e liberdades civis acima mencionadas:

Governança do risco de segurança cibernética

- A avaliação de uma organização sobre o risco de segurança cibernética e respostas a riscos potenciais considera as implicações de privacidade de seu programa de segurança cibernética.
- Indivíduos com responsabilidades relacionadas à segurança cibernética se reportam à gerência apropriada e são devidamente treinados.
- Existe um processo para apoiar *compliance* das atividades de segurança cibernética com as leis de privacidade, regulamentos e requisitos constitucionais aplicáveis.
- Existe um processo para avaliar a implementação das medidas e controles organizacionais acima.

Abordagens para identificar, autenticar e autorizar indivíduos para acessar os ativos e sistemas organizacionais

- Medidas são tomadas para identificar e tratar as implicações de privacidade do gerenciamento de identidades e das medidas de controle de acesso, na medida em que envolvem coleta, divulgação ou uso de informações pessoais.

Medidas de conscientização e treinamento

- As informações aplicáveis das políticas de privacidade organizacional estão incluídas nas atividades de treinamento e conscientização da força laboral

envolvida na segurança cibernética.
- Os provedores de serviços que fornecem serviços relacionados à segurança cibernética para a organização são informados sobre as políticas de privacidade aplicáveis da organização.

Detecção de atividade anômala e monitoramento de sistemas e ativos

- Existe um processo em vigor para conduzir uma avaliação de privacidade do monitoramento de segurança cibernética e de detecção de atividades anômalas de uma organização.

Atividades de resposta, incluindo compartilhamento de informações ou outros esforços de mitigação

- Existe um processo para avaliar e tratar se, quando, como e até que ponto as informações pessoais são compartilhadas fora da organização como parte das atividades de compartilhamento de informações de segurança cibernética.
- Existe um processo em vigor para conduzir uma análise de privacidade dos esforços de mitigação de segurança cibernética de uma organização.

4.0 Autoavaliação do Risco de Segurança Cibernética através do Guia

O Guia da Segurança Cibernética é projetado para reduzir o risco através do aperfeiçoamento do gerenciamento do risco de segurança cibernética de acordo com os objetivos organizacionais. Idealmente, as organizações que usam o Guia serão capazes de medir e atribuir valores ao seu risco *juntamente com* o custo e os benefícios das medidas tomadas para reduzir o risco a níveis aceitáveis. Quanto melhor uma organização for capaz de medir seus riscos, custos e benefícios de estratégias e etapas de segurança cibernética, mais racional, eficaz e valiosa será sua abordagem de segurança cibernética e seus investimentos.

Com o passar do tempo, a autoavaliação e a medição devem melhorar a tomada de decisões acerca das prioridades de investimento. Por exemplo, a medição — ou pelo menos a caracterização robusta — de aspectos do estado de segurança cibernética e tendências da organização ao longo do tempo pode permitir que a organização compreenda e transmita informações significativas sobre riscos para dependentes, fornecedores, compradores e outras partes. Uma organização pode realizar isso internamente ou através de uma avaliação de terceiros. Se feitas corretamente e com um reconhecimento de suas limitações, essas medidas podem fornecer uma base para relacionamentos confiáveis mais fortes, tanto dentro como fora de uma organização.

Para examinar a eficácia dos investimentos, uma organização deve primeiramente ter uma compreensão clara de seus objetivos organizacionais, a relação entre esses objetivos e os resultados de apoio de segurança cibernética, e como esses resultados discretos de segurança cibernética são implementados e gerenciados. Embora as medições de todos esses itens estejam fora do escopo do Guia, os resultados da segurança cibernética da Estrutura Básica dão suporte à autoavaliação da eficácia do investimento e das atividades de segurança cibernética das seguintes maneiras:

- Fazer escolhas sobre como diferentes partes da operação de segurança cibernética devem influenciar a seleção dos Níveis de Implementação Desejados.

- Avaliar a abordagem da organização quanto ao gerenciamento de riscos de segurança cibernética, determinando os Níveis de Implementação Atuais,

- Priorizar os resultados de segurança cibernética através do desenvolvimento de Avaliações Desejadas,
- Determinar o grau em que cada etapa específica de segurança cibernética alcança os resultados desejados de segurança cibernética, analisando Avaliações Atuais, e
- Avaliar o grau de implementação de catálogos de controles ou orientação técnica listados como Referências Informativas.

O desenvolvimento de métricas de desempenho de segurança cibernética está evoluindo. As organizações devem ser cuidadosas, criativas e atentas sobre as maneiras como empregam medições para otimizar o uso, evitando a dependência de indicadores artificiais do estado atual e do progresso na melhoria do gerenciamento de riscos de segurança cibernética. Julgar o risco cibernético requer disciplina e este deve ser reavaliado periodicamente. Sempre que forem utilizadas medições como parte do processo do Guia, as organizações são incentivadas a identificar e saber claramente por que essas medidas são importantes e como elas contribuirão para o gerenciamento global do risco de segurança cibernética. Elas também devem ser claras sobre as limitações das medições que são usadas.

Por exemplo, o monitoramento de medidas de segurança e resultados de negócio podem fornecer uma percepção significativa sobre como as alterações nos controles granulares de segurança afetam o cumprimento dos objetivos organizacionais. A verificação do alcance de alguns objetivos organizacionais requer a análise dos dados somente *depois* que esse objetivo tiver sido alcançado. Esse tipo de medida atrasada é mais verdadeiro. No entanto, muitas vezes é mais valioso prever se um risco de segurança cibernética *pode* ocorrer e o impacto que isso *pode* ter, usando uma medida de liderança.

As organizações são incentivadas a inovar e personalizar a forma como incorporam as medições na sua aplicação do Guia, com uma apreciação completa da sua utilidade e limitações.

Anexo A: Estrutura Básica

Este anexo apresenta a Estrutura Básica: uma lista de Funções, Categorias, Subcategorias e Referências Informativas que descrevem atividades específicas de segurança cibernética que são comuns em todos os setores de infraestrutura crítica. O formato de apresentação escolhido para a Estrutura Básica não sugere uma ordem de implementação específica ou sugere um grau de importância das Categorias, Subcategorias e Referências Informativas. A Estrutura Básica apresentada neste apêndice representa um conjunto comum de atividades para gerenciar o risco de segurança cibernética. Embora o Guia não seja exaustivo, ele é extensível, permitindo que as organizações, os setores e outras entidades usem Subcategorias e Referências Informativas complementares que sejam econômicas e eficientes e que lhes permitam gerenciar seus riscos de segurança cibernética. As atividades podem ser selecionadas a partir da Estrutura Básica durante o processo de criação da Avaliação e outras Categorias, Subcategorias, e Referências Informativas podem ser adicionadas à Avaliação. Os processos de gerenciamento de riscos de uma organização, os requisitos legais/regulatórios, os objetivos de negócios/missão e as restrições organizacionais norteiam a seleção dessas atividades durante a criação da Avaliação. As informações pessoais são consideradas um componente de dados ou ativos referenciados nas Categorias ao avaliar os riscos e proteções de segurança.

Embora os resultados pretendidos identificados nas Funções, Categorias e Subcategorias sejam os mesmos para TI e ICS, os ambientes operacionais e considerações para TI e ICS diferem. A Segurança Cibernética Industrial (ICS, em inglês) têm um efeito direto no mundo físico, incluindo riscos potenciais à saúde e segurança dos indivíduos e impacto no meio ambiente. Além disso, a ICS possui requisitos exclusivos de desempenho e confiabilidade em comparação à TI, e as metas de segurança e eficiência devem ser consideradas ao implementar medidas de segurança cibernética.

Para facilitar o uso, cada componente da Estrutura Básica recebe um identificador exclusivo. Cada uma das Funções e Categorias possui um identificador alfabético único, conforme mostrado na Tabela 1. As Subcategorias dentro de cada categoria são referenciadas numericamente; o identificador exclusivo para cada Subcategoria está incluído na Tabela 2.

Material de apoio adicional, incluindo Referências Informativas, relativo ao Guia pode ser encontrado no site do NIST em http://www.nist.gov/cyberframework/.

Tabela 1: Identificadores Exclusivos de Função e Categoria

Identificador Exclusivo de Função	Função	Identificador Exclusivo de Categoria	Categoria
ID	Identificar	ID.AM	Gerenciamento dos Ativos
		ID.BE	Contexto Empresarial
		ID.GV	Governança
		ID.RA	Avaliação de Risco
		ID.RM	Estratégia de Gerenciamento de Riscos
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimento
PR	Proteger	PR.AC	Gerenciamento de identidade e controle de acesso
		PR.AT	Conscientização e Treinamento
		PR.DS	Segurança de Dados
		PR.IP	Processos e Procedimentos de Proteção da Informação
		PR.MA	Manutenção
		PR.PT	Tecnologia Protetora
DE	Detectar ou Diagnosticar	DE.AE	Anomalias e Incidentes
		DE.CM	Monitoramento Contínuo de Segurança
		DE.DP	Processos de Detecção
RS	Responder	RS.RP	Planejamento de Resposta
		RS.CO	Comunicações
		RS.AN	Análise
		RS.MI	Mitigação
		RS.IM	Aperfeiçoamentos
RC	Recuperar	RC.RP	Planejamento de Recuperação
		RC.IM	Aperfeiçoamentos
		RC.CO	Comunicações

Tabela 2: Estrutura Básica

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)	**Gerenciamento de Ativos (ID.AM):** Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos de negócio são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.	**ID.AM-1:** Dispositivos físicos e sistemas dentro da organização são inventariados	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR. 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Plataformas de software e aplicações dentro da organização são inventariadas	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR. 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Comunicação organizacional e fluxos de dados são mapeados	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, 3-CA, CA-9, PL-8
		ID.AM-4: Sistemas de informação externos são catalogados	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Função	Categoria	Subcategoria	Referências Informativas
	Contexto Empresarial (ID.BE): A missão, objetivos, *stakeholders* e atividades da organização são compreendidos e priorizados; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.	**ID.BE-1:** O papel da organização na cadeia de suprimentos é identificado e comunicado	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** M-11, SA-14
		ID.BE-4: Dependências e funções críticas para a entrega de serviços críticos são estabelecidas	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos as condições operacionais (por exemplo, sob coerção/ ataque, durante a recuperação, operações normais)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA- 14
	Governança (ID.GV): As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulatórios, jurídicos, de risco, ambientais e operacionais da organização são compreendidos e informam gerenciamento do risco de segurança cibernética.	**ID. GV-1:** A política organizacional de segurança cibernética é estabelecida e comunicada	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 4 Rev.** -1 controles de todas as famílias de controle de segurança

Função	Categoria	Subcategoria	Referências Informativas
		ID.GV-2: As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 4 Rev.** -1 controles de todas as famílias de controle de segurança
		ID.GV-4: Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Cláusula 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, 7-PM, PM-9, 10 PM, PM-11
	Avaliação de risco (ID.RA): A organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos.	**ID.RA-1:** As vulnerabilidades dos ativos são identificadas e documentadas	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

Função	Categoria	Subcategoria	Referências Informativas
		ID.RA-3: Ameaças internas e externas são identificadas e documentadas	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM- 16
		ID.RA-4: Potenciais impactos no negócio e probabilidades são identificados na organização	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM- 9, PM-11
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: As respostas ao risco são identificadas e priorizadas	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Estratégia de Gerenciamento de Riscos (ID.RM): As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.	**ID.RM-1:** Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos *stakeholders* organizacionais	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001: 2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Tolerância ao risco organizacional é determinada e claramente expressa	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** PM-9

Função	Categoria	Subcategoria	Referências Informativas
		ID.RM-3: A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 AP 4** SA-14, PM-8, PM-9 PM-11
	Gerenciamento de Riscos da Cadeia de Suprimento (ID.SC): As prioridades, restrições, tolerâncias de risco e suposições da organização são definidas e utilizadas para apoiar as decisões de risco associadas ao gerenciamento do risco da cadeia de suprimentos. A organização definiu e implementou os processos para identificar, avaliar e gerenciar os riscos da cadeia de suprimentos.	**ID.SC-1:** Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA- 14, SA-15, PM-9
		ID.SC-3: Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, 9 PM

Função	Categoria	Subcategoria	Referências Informativas
		ID.SC-4: Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3: 2013** SR 2.8, SR 3.3, SR.6.1, SR-7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, 3-IR, IR-4, 6-IR, IR-8, IR-9
PROTEGER (PR)	**Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC):** O acesso a ativos físicos e lógicos e recursos associados é limitado a usuários, processos e dispositivos autorizados e é gerenciado de maneira consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas.	**PR.AC-1:** Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR-1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 e3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

Função	Categoria	Subcategoria	Referências Informativas
		PR.AC-3: O acesso remoto é gerenciado	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, 19-AC, AC-20, SC-15
		PR.AC-4: Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, 16-AC, AC-24
		PR.AC-5: A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: As identidades são revisadas, vinculadas a credenciais e confirmadas em interações	**CIS CSC** ,16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR-1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, 4-IA, IA-5, IA-8, PE-2, PS-3

Função	Categoria	Subcategoria	Referências Informativas
		PR.AC-7: Usuários, dispositivos e outros recursos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Conscientização e Treinamento (PR.AT): Os funcionários e parceiros da organização são treinados sobre a conscientização sobre segurança cibernética e são treinados para executar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com os procedimentos e acordos relacionados.	**PR.AT-1:** Todos os utilizadores são informados a respeito e treinados	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Os usuários privilegiados compreendem suas funções e responsabilidades	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: *Stakeholders* terceirizados (por exemplo, fornecedores, clientes, parceiros) entendem suas funções e responsabilidades	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Executivos seniores compreendem suas funções e responsabilidades	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13

Função	Categoria	Subcategoria	Referências Informativas
		PR.AT-5: Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades	**CIS CSC** 17 **COBIT** 5 APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Segurança de Dados (PR.DS): As informações e os registros (dados) são gerenciados de maneira consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade de informações.	**PR.DS-1:** Os dados em repouso são protegidos	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, 12-SC, SC-28
		PR.DS-2: Os dados em trânsito são protegidos	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Ativos são formalmente gerenciados durante a remoção, transferências e disposição	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: A capacidade adequada para garantir a disponibilidade é mantida	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: As proteções contra vazamentos de dados são implementadas	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2,

Função	Categoria	Subcategoria	Referências Informativas
			A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, 7-SC, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do hardware	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.2.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Processos e Procedimentos de Proteção da Informação (PR.IP): As políticas de segurança (que abordam a finalidade, o escopo, as funções, as responsabilidades, o compromisso de gerenciamento e a coordenação entre as entidades organizacionais), processos e procedimentos são mantidas e usadas para gerenciar a proteção de sistemas e ativos de informações.	**PR.IP-1:** Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR. 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1 A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17

Função	Categoria	Subcategoria	Referências Informativas
		PR.IP-3: Processos de controle de mudança de configuração estão em funcionamento	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR. 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Os Backups de informações são realizados, conservados e testados	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Os dados são destruídos de acordo com a política	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Os processos de proteção são aperfeiçoados	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO / IEC 27001: 2013** A.16.1.6 Cláusula 9, Cláusula 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

Função	Categoria	Subcategoria	Referências Informativas
		PR.IP-8: A eficácia das tecnologias de proteção é compartilhada	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados	**CIS CSC** 19 **COBIT 5** APO11.06, APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, 7-CP, CP-12, CP-13, IR-7, 8-IR, IR-9, PE-17
		PR.IP-10: Planos de recuperação e resposta são testados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, 7-PS, PS-8, SA-21
		PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013**A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Manutenção (PR.MA): A manutenção e os reparos de componentes de sistemas de controle e informações industriais são executados de acordo com políticas e procedimentos.	**PR. MA-1:** Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 MA **de Rev. 4-2,** NIST SP 800-53 MA-3, 5-MA, MA-6

Função	Categoria	Subcategoria	Referências Informativas
		PR.MA-2: A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Tecnologia Protetora (PR.PT): As soluções de segurança técnica são gerenciadas para garantir a segurança e resiliência de sistemas e ativos, consistentes com políticas, procedimentos e acordos relacionados.	**PR.PT-1:** Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR-2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Família
		PR.PT-2: As mídias removíveis são protegidas e seu uso é restrito de acordo com a política	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2 MP-3, MP-4, MP -5, MP-7, MP-8
		PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR-1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR-1.10, SR 1.11 SR 1.12, SR. 1.13, SR 2.1, SR 2.2, SR-2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7

Função	Categoria	Subcategoria	Referências Informativas
		PR.PT-4: Redes de comunicação e controle são protegidas	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR-4.1, SR 4.3, SR 5.1, 5.2 de SR, SR 5.3, SR 7.1, SR 7,6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, 25-SC, SC-29, SC-32, SC-36, 37-SC, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Alguns mecanismos (por exemplo*, fail-safe, load balancing, hot swap*) são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECTAR (DE)	**Anomalias e Incidentes (DE.AE):** Atividade anômala é detectada e o impacto potencial dos eventos é compreendido.	**DE.AE-1:** Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR-2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4

Função	Categoria	Subcategoria	Referências Informativas
		DE.AE-1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR-2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: O impacto dos eventos é determinado	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Os limites de alerta de incidentes são estabelecidos	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Monitoramento Contínuo de Segurança (DE.CM): O sistema de informação e os ativos são monitorados para identificar incidentes de segurança cibernética e verificar a eficácia das medidas de proteção.	**DE.CM-1:** A rede é monitorada para detectar potenciais incidentes de segurança cibernética	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM- 3, SC-5, SC-7, SI-4

Função	Categoria	Subcategoria	Referências Informativas
		DE.CM-2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Código malicioso é detectado	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Código móvel não autorizado é detectado	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.15.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, 6-PE, PE-20, SI-4
		DE.CM-8: Há realização de varreduras de vulnerabilidade	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5

Função	Categoria	Subcategoria	Referências Informativas
	Processos de Detecção (DE.DP): Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização sobre eventos anômalos	**DE.DP-1:** Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas	**CIS CSC** 19 **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA- 18, SI-4, PM-14
		DE.DP-3: Os processos de detecção são testados	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Informações de detecção de incidente são comunicadas	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA- 5, SI-4
		DE.DP-5: Processos de detecção são continuamente aperfeiçoados	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14
RESPONDER (RS)	**Planejamento de Respostas (RS.RP):** Os processos e procedimentos de resposta são executados e mantidos para garantir a resposta a incidentes de segurança cibernética detectados.	**RS.RP-1:** Plano de resposta é executado durante ou depois de um incidente	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8

Função	Categoria	Subcategoria	Referências Informativas
	Comunicações (RS.CO): As atividades de resposta são coordenadas com *stakeholders* internos e externos (por exemplo, apoio externo de órgãos fiscalizadores)	**RS.CO-1:** Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Os incidentes são informados de acordo com os critérios estabelecidos	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: As informações são compartilhadas de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: A coordenação com os *stakeholders* ocorre de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
		RS.CO-5: O compartilhamento voluntário de informações ocorre com os *stakeholders* externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Função	Categoria	Subcategoria	Referências Informativas
	Análise (RS.AN): A análise é realizada para garantir resposta eficaz e dar apoio às atividades de recuperação.	**RS.AN-1:** As notificações dos sistemas de detecção são analisadas	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: O impacto do incidente é compreendido	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Há realização de investigações	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Os incidentes são categorizados de forma consistente com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança).	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Função	Categoria	Subcategoria	Referências Informativas
	Mitigação (RS.MI): As atividades são realizadas para impedir a expansão de um evento, atenuar seus efeitos e resolver o incidente.	**RS.MI-1: Os** incidentes são contidos	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Os incidentes são mitigados	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Aperfeiçoamentos (RS.IM): As atividades de resposta organizacionais são aperfeiçoadas pela incorporação de lições aprendidas de atividades anteriores de detecção/resposta.	**RS.IM-1: Os** planos de resposta incorporam as lições aprendidas	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
		RS.IM-2: As estratégias de resposta são atualizadas	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
RECUPERAR (RC)	**Planejamento de Recuperação (RC.RP):** Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração de sistemas ou ativos afetados por incidentes de segurança cibernética.	**RC.RP-1:** O Plano de recuperação é executado durante ou após um incidente de segurança cibernética	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

Função	Categoria	Subcategoria	Referências Informativas
	Aperfeiçoamentos (RC.IM): O planejamento e os processos de recuperação são aperfeiçoados pela incorporação de lições aprendidas em atividades futuras	**RC. IM-1:** Planos de recuperação incorporam as lições aprendidas	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
		RC.IM-2: As estratégias de recuperação são atualizadas	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, provedores de serviços de Internet, proprietários de sistemas de ataque, vítimas, outras CSIRTs e fornecedores).	**RC.CO-1:** As relações públicas são gerenciadas	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4
		RC.CO-2: A reputação é reparada após um incidente	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cláusula 7.4
		RC.CO-3: As atividades de recuperação são comunicadas aos *stakeholders* internos e externos, bem como às equipes executivas e de gestão.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Informações sobre Referências Informativas descritas no Anexo A podem ser encontradas em:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1(99.02.01)-2009,*Security for Industrial Automation and Control Systems: Estabelecendo um Programa de Segurança de Sistemas de Controle e Automação Industrial*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013,*Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001,*Information technology -- Security techniques -- Information security managementsystems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4,*Security and PrivacyControls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Referências informativas são mapeadas apenas para o nível de controle, embora qualquer aprimoramento de controle possa ser considerado útil na obtenção de um resultado de subcategoria.

Os mapeamentos entre as Subcategorias da Estrutura Básica e as seções especificadas nas Referências Informativas não têm a intenção de determinar definitivamente se as seções especificadas nas Referências Informativas fornecem o resultado da Subcategoria desejado.

As Referências Informativas não são exaustivas, pois nem todos os elementos (por exemplo, controle, requisito) de uma determinada Referência Informativa são mapeados para as Subcategorias da Estrutura Básica.

Anexo B: Glossário

Neste anexo você encontrará os significados dos termos utilizados nesta publicação

Tabela 3: Glossário do Guia

Comprador	As pessoas ou organizações que consomem determinado produto ou serviço.
Categoria	A subdivisão de uma função em grupos de resultados de segurança cibernética, intimamente ligada as necessidades programáticas e atividades específicas. Exemplos de Categorias incluem "Gerenciamento de ativos", "Gerenciamento de identidades e controle de acesso" e "Processos de detecção".
Infraestrutura Crítica	Sistemas e ativos, físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição desses sistemas e ativos teria um impacto debilitante na segurança cibernética, segurança econômica nacional, saúde pública nacional ou segurança, ou qualquer combinação dessas áreas.”
Segurança Cibernética	O processo de proteção de informações prevenindo, detectando e respondendo a ataques.
Evento de Segurança Cibernética	Uma alteração de segurança cibernética que pode ter um impacto sobre as operações organizacionais (incluindo a missão, recursos ou reputação).
Incidentes de Segurança Cibernética	Um evento de segurança cibernética que foi determinado como tendo um impacto na organização, levando à necessidade de resposta e recuperação.
Detectar (função)	Desenvolver e implementar as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética.
Guia	O Guia é uma abordagem baseada no conhecimento de risco para auxiliar o gerenciamento de risco de segurança cibernética e é composto por três partes: a Estrutura Básica, os Níveis de Implementação da Estrutura e as Avaliações da Estrutura.
Estrutura Básica	Conjunto de atividades de segurança cibernética e referências que são comuns em setores de infraestrutura crítica e são organizadas em torno de resultados específicos. A Estrutura Básica é composta por quatro tipos de elementos: Funções, Categorias, Subcategorias e Referências Informativas.

Níveis de Implementação	Uma lente através da qual é possível visualizar as características da abordagem de risco de uma organização — como uma organização vê o risco de segurança cibernética e os processos em vigor para gerenciar esse risco.
Avaliação da Estrutura	Uma representação dos resultados que um determinado sistema ou organização selecionou das Categorias e Subcategorias do Guia.
Função	Um dos principais componentes do Guia. As funções fornecem o nível mais alto de estrutura para organizar atividades básicas de segurança cibernética em Categorias e Subcategorias. Essas funções são Identificar, Proteger, Detectar, Responder e Recuperar.
Identificar (função)	Identificar — Desenvolve uma compreensão organizacional para gerenciar o risco de segurança cibernética para sistemas, pessoas, ativos, dados e recursos.
Referências Informativas	Uma seção específica de normas, diretrizes e práticas comuns entre os setores de infraestrutura crítica que ilustram um método para alcançar os resultados associados a cada Subcategoria. Um exemplo de uma Referência Informativa é o Controle ISO/IEC 27001 A.10.8.3, que suporta a Subcategoria “Dados em trânsito estão protegidos” da categoria “Segurança de Dados” na função “Proteger”.
Código Móvel	Um programa (por exemplo, script, macro ou outra instrução portátil) que pode ser enviado inalterado para uma coleção heterogênea de plataformas e executado com semântica idêntica.
Proteger (função)	Desenvolve e implementa as proteções apropriadas para garantir a entrega de serviços críticos de infraestrutura.
Usuário Privilegiado	Um usuário que está autorizado (e, portanto, confiável) a executar funções relevantes para a segurança que usuários comuns não estão autorizados a executar.
Recuperar (função)	Desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um evento de segurança cibernética.
Responder (função)	Desenvolver e implementar as atividades apropriadas para agir em relação a um evento de segurança cibernética detectado.

Risco	Uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento em potencial, e tipicamente uma função de: (i) os impactos adversos que surgiriam se a circunstância ou evento ocorresse; e (ii) a probabilidade de ocorrência.
Gerenciamento de Risco	O processo de identificação, avaliação e resposta ao risco.
Subcategoria	A subdivisão de uma Categoria em resultados específicos de atividades técnicas e/ou de gestão. Exemplos de subcategorias incluem "Sistemas externos de Informação estão catalogados", "Dados em repouso estão protegidos" e "Notificações de sistemas de detecção são investigadas".
Fornecedor	Provedores de produtos e serviços usados para fins internos de uma organização (por exemplo, infraestrutura de TI) ou integrados aos produtos de serviços fornecidos aos Compradores dessa organização.
Taxonomia	Um esquema de classificação.

Anexo C: Acrônimos

Neste anexo você encontrará os significados dos termos utilizados nesta publicação

ANSI	Instituto Nacional de Padrões Americanos (*American National Standards Institute, em inglês*)
CEA	Lei de Aprimoramento da Segurança Cibernética de 2014 (*Cybersecurity Enhancement Act of 2014*)
CIS	Centro de Segurança da Internet *(Center for Internet Security)*
COBIT	Objetivos de Controle para Informação e Tecnologia Relacionada *(Control Objectives for Information and Related Technology)*
CPS	Sistemas ciber-físicos *(Cyber-Physical Systems)*
CSC	Controle de segurança crítica *(Critical Security Control)*
DHS	Departamento de Segurança Interna *(Department of Homeland Security)*
EO	Ordem Executiva ou Decreto
ICS	Sistemas de Controle Industrial *(Industrial Control Systems)*
IEC	Comissão Eletrotécnica Internacional *(International Electrotechnical Commission)*
IoT	Internet das Coisas
IR	Relatório Interagencial
ISA	Sociedade Internacional de Automação
ISAC	Centro de Compartilhamento e Análise de Informações
ISAO	Organização de Compartilhamento e Análise de Informações
ISO	Organização Internacional para Padronização
IT	Tecnologia da Informação
NIST	Instituto Nacional de Padrões e Tecnologia
OT	Tecnologia operacional
PII	Informação Pessoal Identificável
RFI	Pedido de Informações
RMP	Processo de Gerenciamento de Riscos
SCRM	Gerenciamento de riscos em cadeias de suprimentos

U.S. CHAMBER OF COMMERCE

1615 H STREET NW WASHINGTON, DC 20062, USA | USCHAMBER.COM