Presidência da República

Comitê Nacional de Cibersegurança (CNCiber)

Modelo de Ciber-Maturidade Brasileiro – Institucional (CIMBRA-I)

(v1)

Brasília - 2026

SUMÁRIO

1 APRESENTAÇÃO

1.1 Introdução

Com o objetivo de permitir uma melhor consciência situacional da realidade da cibersegurança e da ciber-resiliência brasileiras o Comitê Nacional de Cibersegurança (CNCiber) criou um Grupo de Trabalho Temático (GTT) para elaborar dois modelos de maturidade em cibersegurança adequados às condições brasileiras: um de avaliação das condições nacionais e outro de avaliação das condições institucionais em instituições públicas e privadas de diferentes setores da sociedade.

O início das atividades do GTT Maturidade foi pautado pelo nivelamento técnico e conceitual necessário para a realização da tarefa delegada ao grupo. Foram estudados conceitos de modelos, arcabouços (frameworks), maturidade e conformidade, e modelos prescritivos e descritivos. Foram estudados ainda diversos modelos e arcabouços (*frameworks*), tanto de maturidade quanto de conformidade, ou até de boas práticas, envolvendo as mais variadas temáticas ligadas à cibersegurança, passando pela segurança da informação, desenvolvimento de software, governança de TI, que pudessem prover elementos a serem incorporados à proposta de modelos de avaliação da maturidade brasileira em cibersegurança, nacional ou institucional.

2 O MODELO CIBERMATURIDADE BRASILEIRA – CIMBRA

Após o nivelamento técnico-conceitual dos integrantes do GTT e a pesquisa dos modelos e arcabouços mais usados internacionalmente, decidiu-se que a proposta seria fundamentada em um mix de características de diferentes origens, cujo detalhamento é apresentado nos próximos capítulos.

2.1 O que é uma “cimbra”

Cimbra é uma palavra usada em português e espanhol para designar uma estrutura de madeira ou metal usada para fazer arcos, abóbadas, lajes ou vigas. Portanto, um elemento estruturante que suporta a construção de armações permanentes de longa duração.

Suas principais funções são:

- Sustentação: Suporta o peso do concreto fresco, das fôrmas, dos equipamentos e dos operários até que a estrutura atinja a resistência necessária.
- Moldagem: Mantém a geometria correta do projeto (curvaturas de arcos, nivelamento de lajes, etc.).
- Segurança: Garante que a estrutura não sofra deformações ou desabamentos durante a fase crítica de cura do concreto.

É uma palavra curta, com sentido próprio, associável à contração da denominação Ciber Maturidade Brasileira.

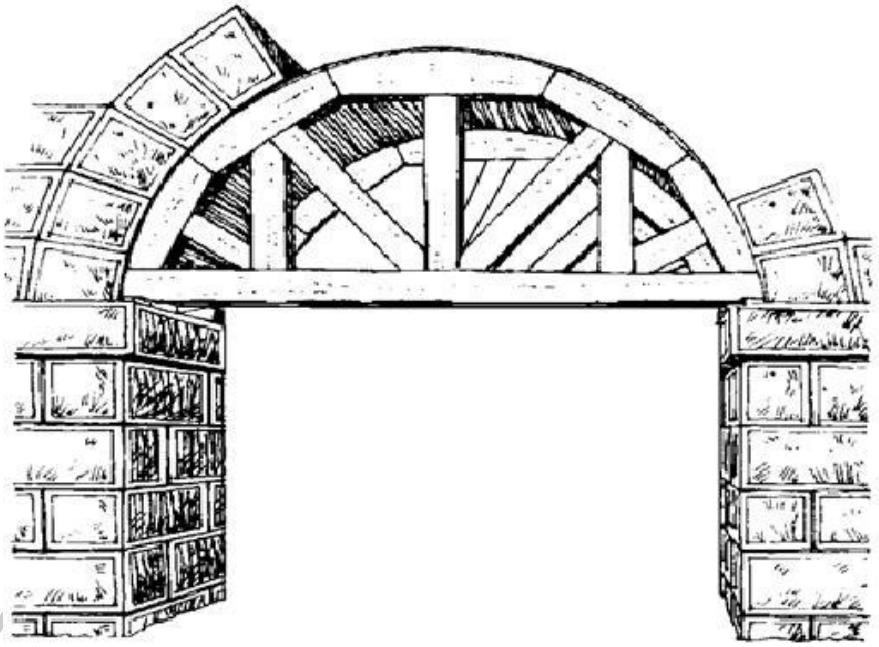


Figura 1- Exemplo de Cimbra

Por essas razões o nome CIMBRA foi adotado pelo GTT para o Modelo de Ciber Maturidade Brasileiro. Suas duas variantes seriam:

- Cimbra-Nacional (ou Cimbra-N): tem como finalidade a mensuração da maturidade nacional em cibersegurança ao longo do tempo, permitindo identificar pontos fortes, fracos e de atenção, que possam representar riscos ou oportunidades para a cibersegurança do País.
- Cimbra-Institucional (ou Cimbra-I): tem por finalidade a mensuração da maturidade institucional em cibersegurança, refletindo o grau de implementação das diferentes práticas em instituições de diferentes setores e portes, públicas ou privadas. A análise de informações de instituições de um mesmo setor permitirá o mapeamento da maturidade setorial em cibersegurança.

3 A ESCALA DE MATURIDADE

A escala de maturidade do CIMBRA foi estruturada com 6 <Níveis> (estágios) aplicáveis cumulativamente:

Nível	Características de Gestão	Características de Abordagem
0-Inicial	As <Práticas> não são realizadas	Não são identificáveis evidências de implementações de todas as <Práticas> exigidas para o nível Fundamental
1-Fundamental	As <Práticas> são realizadas, mas podem ser ad hoc, sem coordenação central	São identificáveis implementações básicas de todas as <Práticas> classificadas como nível Fundamental, e possivelmente de algumas práticas do nível Médio
2-Básico	As <Práticas> são formalizadas e documentadas	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental e Médio, e possivelmente de algumas práticas do nível Evoluído.

Nível	Características de Gestão	Características de Abordagem
3-Médio	As <Práticas> são guiadas por políticas (ou outras diretrizes organizacionais) Recursos adequados são fornecidos para apoiar o <Processo>	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental e Médio, e possivelmente de algumas práticas do nível Evoluído.
4-Evoluído	Responsabilidade, prestação de contas e autoridade pela execução das <Práticas> são atribuídas Implementações são guiadas por prioridades e análise de riscos O pessoal que executa as <Práticas> tem habilidades e conhecimentos adequados e verificados	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental, Médio e Evoluído, e possivelmente de algumas práticas do nível Avançado.
5-Avançado	A eficácia das <Práticas> é avaliada e rastreada Políticas, <Processos> e <Práticas> são aprimoradas com base em lições aprendidas, de forma sistemática, indicando capacidade de adaptação rápida a novas ameaças	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental, Médio, Evoluído e Avançado.

Tabela 1 – Níveis de Maturidade do CIMBRA

No contexto do CIMBRA observou-se a característica cumulativa dos níveis de maturidade, segundo a qual a progressão entre níveis ocorre de forma sequencial e condicionada. Isso significa que o atingimento de um <Nível> de maturidade subsequente está necessariamente vinculado à plena implementação e à evidência objetiva de todas as práticas, controles e requisitos estabelecidos para o <Nível> imediatamente anterior.

Dessa forma, assegura-se consistência evolutiva, consolidação das capacidades institucionais e a construção estruturada de competências ao longo do tempo, evitando lacunas ou sobreposições no desenvolvimento do modelo.

Como exemplo hipotético, pode-se citar a situação em que se demande a existência de Planos Setoriais elaborados pelas autoridades reguladoras setoriais para se atingir o <Nível> Evoluído de maturidade. Se um único setor regulado não dispuser desse plano setorial o país tem sua avaliação prejudicada nesse quesito, pois não terá cumprido a exigência e não há uma ponderação do quesito.

4 HIERARQUIA EM 3 NÍVEIS

O Cimbra-I teve como referência básica o *Cyber Capability Maturity Model* (C2M2), elaborado pelo Departamento de Energia dos EUA, o *Cybersecurity Framework* (CSF) 2.0, elaborado pelo *National Institute of Standards and Technology* (NIST) dos EUA, e o Programa de Privacidade e Segurança da Informação (PPSI) 2.0, elaborado pelo Governo Brasileiro, incorporando elementos entendidos como relevantes derivados dos demais modelos de referência: COBIT, ITIL, CIS e ISO.

Foi elaborado com uma estrutura baseada em 3 níveis hierarquizados conforme se segue.

4.1 <Eixo>

Um <Eixo> representa um domínio do conhecimento, a categoria que agrupa capacidades relacionadas. Partindo-se das estruturas dos modelos e arcabouços considerados, entendeu-se pela estruturação do CIMBRA-I baseado em 14 <Eixos> temáticos.

4.2 <Processo>

Um <Processo> é um conjunto de <Ações> articuladas dentro de um <Eixo>.

4.3 <Ação>

Uma <Ação> consiste no nível mais granular e operacional da hierarquia, indicando "o quê" deve ser feito para se implementar um <Processo>. É nesse nível que será avaliada a maturidade da execução das <Práticas> de cibersegurança que compõem o CIMBRA-I.

5 CONFIGURAÇÃO

O CIMBRA-I foi idealizado de forma a permitir <Configurações> flexíveis do modelo para diferentes realidades. Essencialmente, uma <Configuração> é uma associação das <Ações> com os níveis de <Maturidade> buscados para <Instituições> com determinada característica.

No contexto de instituições prestadoras de Serviços Essenciais ou operadoras de Infraestruturas Críticas, por exemplo, uma <Configuração> do CIMBRA-I pode ser vinculada à <Essencialidade> das instituições de determinado setor. Dessa forma, a autoridade reguladora setorial pode estipular que determinada <Ação> terá níveis de exigência distintos para instituições com Essencialidades diferentes em seu setor regulado.

Essa característica do CIMBRA-I atribui ao modelo uma elevada adaptabilidade a instituições de diferentes portes em diferentes contextos setoriais e momentos no tempo, mantendo a coesão do modelo e permitindo um processo de amadurecimento guiado e acompanhado em ritmos diverso para cada setor, a critério da autoridade reguladora setorial.

6 A ESCALA DE ESSENCIALIDADE DE SERVIÇOS

Com foco na resiliência de serviços essenciais, é necessário observar que existe uma escala de Essencialidade de serviços que pode variar de acordo com diferentes parâmetros.

6.1 Níveis de Essencialidade

E escala de essencialidade do CIMBRA foi estruturada com 5 <Níveis>.

Nível	Características
1-Complementar	A interrupção tem impacto limitado
2-Importante	A interrupção gera inconveniência contornável
3-Relevante	A interrupção tem impacto significativo, com alternativas caras ou lentas
4-Crítica	A interrupção causa impactos severos em poucas horas
5-Vital	A interrupção causa colapso imediato ou riscos à vida/segurança nacional

Tabela 2 – Níveis de Essencialidade do CIMBRA

6.2 Critérios de Determinação da Essencialidade

No contexto do CIMBRA-I foram considerados os seguintes critérios para determinação da essencialidade de serviços:

6.2.1 Alcance (Usuários Alcançados)

Nível	Características
1-Complementar	O Serviço afeta até 50.000 usuários
2-Importante	O Serviço afeta até 100.000 usuários
3-Relevante	O Serviço afeta até 250.000 usuários

Nível	Características
4-Crítica	O Serviço afeta até 500.000 usuários
5-Vital	O Serviço afeta mais de 500.000 usuários

Tabela 3 – Exemplo de definição da Essencialidade com base no número de usuários

Obs.: os números apresentados na Tabela 3 são apenas ilustrativos, podendo ser adaptados conforme a conveniência do ORS responsável pela avaliação.

6.2.2 Participação de Mercado

Nível	Características
1-Complementar	A instituição detém participação de mercado até 1%
2-Importante	A instituição detém participação de mercado até 2%
3-Relevante	A instituição detém participação de mercado até 3%
4-Crítica	A instituição detém participação de mercado até 5%
5-Vital	A instituição detém participação de mercado maior que 5%

Tabela 4 – Exemplo de definição da Essencialidade com base na participação de mercado

Obs.: os números apresentados na Tabela 4 são apenas ilustrativos, podendo ser adaptados conforme a conveniência do ORS responsável pela avaliação.

6.2.3 Criticidade da Operação

Nível	Características
1-Complementar	O serviço é comum e existem vários fornecedores equivalentes. A troca é imediata e sem maiores impactos de transição.
2-Importante	Existem alternativas no mercado. A troca exige um esforço administrativo simples e pouco tempo de adaptação
3-Relevante	A substituição é possível, mas demandará meses. Há custos de migração de dados e necessidade de treinamento na nova solução.
4-Crítica	Há poucas alternativas de substituição. A troca é complexa, cara e gera alto risco de indisponibilidade durante a transição.
5-Vital	A substituição é inviável a curto/médio prazo sem colapso do serviço. [considerar definição ligada ao impacto social]

Tabela 5 – Exemplo de definição da Essencialidade com base na criticidade da operação

As Características descritas na Tabela 5 podem ser determinadas discricionariamente pelo ORS conforme o impacto em serviços considerados críticos para determinada situação específica [detalhar].

6.3 Cômputo da Essencialidade

Após a determinação do Nível de cada critério, a Essencialidade geral da instituição será correspondente ao maior nível dentre todos os apurados.

7 AS EVIDÊNCIAS DE MATURIDADE

O Modelo CIMBRA-I foi concebido para que as avaliações sejam baseadas em evidências. Para facilitar o processo de comprovação foi elaborado, a partir da Escala de Maturidade, um conjunto de Exigências, cuja comprovação pode ser apresentada individualmente.

As Exigências associadas a cada Nível de maturidade são listadas na tabela a seguir.

Nível	<Exigências>	Descrição
1-Fundamental	Ad hoc, sem coordenação central	Atividades executadas por iniciativas pessoais, sem demanda ou coordenação central nem ferramental ou procedimentos disponibilizados
2-Básico	Normas e Procedimentos formais	Existem normas ou procedimentos que orientam a execução da <Prática>
3-Médio	Políticas ou diretrizes institucionais	As normas ou procedimentos são alinhadas a políticas ou diretrizes institucionais e não apenas departamentais
3-Médio	Recursos alocados	Recursos (humanos, materiais e financeiros) são alocados para a realização da <Prática>
4-Evoluído	Responsabilização explícita	Existe a designação formal de um responsável pela <Prática>
4-Evoluído	Cobrança instituída	O responsável pela <Prática> é formalmente cobrado pela sua execução (fiscalização, auditoria ou outro modelo de acompanhamento ou controle)
4-Evoluído	Autoridade atribuída	O responsável tem autoridade formalmente instituída para apoiar a execução da <Prática>
4-Evoluído	Habilidades e conhecimentos providos	O responsável recebeu treinamento ou dispõe das habilidades e conhecimentos necessários para a execução da <Prática>
4-Evoluído	Habilidades e conhecimentos verificados	O responsável teve as habilidades e conhecimentos necessários para a execução da <Prática> verificados
4-Evoluído	Implementações guiadas por prioridades	A execução da <Prática> é guiada por prioridades definidas pela alta-gestão da instituição
4-Evoluído	Implementações guiadas por análise de riscos	A execução da <Prática> é guiada por prioridades definidas com base em análise de risco, do mais elevado para o menos elevado
5-Avançado	Eficácia avaliada	A execução da <Prática> tem sua eficácia avaliada periodicamente, comparada com a linha de base das execuções anteriores
5-Avançado	Eficácia rastreada	A execução da <Prática> tem sua eficácia rastreada periodicamente, comparada com a linha de base das execuções anteriores
5-Avançado	<Práticas> aprimoradas	As <Práticas> e sua execução são aprimoradas regularmente
5-Avançado	Lições aprendidas coletadas sistematicamente	Lições aprendidas durante a execução da <Prática> são coletadas sistematicamente e aplicadas na melhoria do <Processo>
5-Avançado	Novas ameaças tratadas sistematicamente	O monitoramento de novas ameaças é sistematicamente incorporado às <Práticas>

Tabela 6 – Exigências associadas a cada nível de maturidade do CIMBRA-I

Apresentadas as evidências para cada <Exigência>, o avaliador tem condições de verificar aquelas cumpridas e indicar possibilidades de melhoria a curto médio e longo prazos para o atingimento das exigências mínimas ou para a elevação da maturidade nas <Ações> de interesse da Instituição.

Observa-se a possibilidade de haja comprovação de atendimento a determinada Exigência de um nível de maturidade mais elevado, mas dada a natureza cumulativa das exigências dos diferentes níveis, o não cumprimento de uma única Exigência de determinado nível elimina a possibilidade de enquadramento da maturidade da instituição naquele nível. Em outros termos, a maturidade final da

Instituição será aquela cuja totalidade das exigências seja atendida, mesmo que parte das exigências do nível subsequente tenha sido atendida.

8 FOCO NO DESENVOLVIMENTO DE CAPACIDADES

A proposta do CIMBRA incorpora tanto uma perspectiva prescritiva quanto uma perspectiva descritiva. Isso porque nos níveis iniciais, onde a maturidade é menor, as instituições costumam ser menores e com menor capacidade de investimento, beneficiando-se de "receitas prontas" para acelerarem seu amadurecimento. No entanto, tradicionalmente, os níveis mais elevados de maturidade em cibersegurança demandam maior customização e adaptação dos <Processos> e <Ações> às diferentes realidades institucionais, conforme o nível de maturidade coloca exigências maiores de governança, controle e resposta, implicando em investimentos mais significativos.

Dessa forma, desenha-se o CIMBRA com a perspectiva de que tenha as seguintes características associadas a cada nível:

Nível	Característica
Inicial	Prescritivo
Fundamental	Prescritivo
Básico	Prescritivo
Médio	Prescritivo
Evoluído	Descritivo
Avançado	Descritivo

Tabela 7 – Modelagem Prescritiva-Descritiva do CIMBRA por Nível de Maturidade

9 DETALHAMENTO DO CIMBRA-INSTITUCIONAL (CIMBRA-I)

Legenda:

Em fundo VERDE são os <Eixos>.

Em fundo AMARELO são os <Processos>.

Em fundo AZUL são as <Ações>.

E01-ATIVOS-TI

Gerenciamento de ativos, alterações e configuração

Resumo:

Um ativo é algo de valor para uma <Instituição>. Para os fins do modelo, os ativos a serem considerados são ativos de hardware e software de TI, bem como informações essenciais para operar a função.

Detalhamento:

Um inventário de ativos importantes para a execução da função é um recurso importante na gestão de ciber-riscos. O registro de informações importantes, como versão do software, localização física, proprietário do ativo e prioridade, possibilita muitas outras <Ações> de gestão de cibersegurança. Por exemplo, um inventário de ativos robusto pode identificar o local de implantação do software que requer aplicação de patches.

Gerenciar a configuração de ativos envolve definir uma linha de base de configuração e garantir que os ativos sejam configurados de acordo com essa linha de base. Normalmente, essa prática se aplica para garantir que ativos semelhantes sejam configurados da mesma maneira. No entanto, nos casos em que os ativos são únicos ou devem ter configurações individuais, o gerenciamento da configuração de ativos envolve o controle da linha de base de configuração.

O gerenciamento de alterações nos ativos inclui a análise das alterações solicitadas para garantir que elas não introduzam vulnerabilidades inaceitáveis no ambiente operacional, garantindo que todas as alterações sigam o processo de gerenciamento de alterações e identificando alterações não autorizadas. O controle de alterações se aplica a todo o ciclo de vida do ativo, incluindo definição de requisitos, testes, implantação e manutenção e desativação da operação.

E01-ATIVOS-TI-01

Gerenciar o inventário de ativos de hardware de TI

E01-ATIVOS-TI-01-A

Os ativos de hardware de TI importantes para a entrega da <Instituição> são inventariados

Detalhamento:

Os ativos obtêm seu valor e importância por meio de sua associação com os aspectos das operações da <Instituição> que suportam. Identificar e inventariar ativos de hardware de TI de alto valor ajuda a possibilitar a seleção e aplicação de controles apropriados. a <Instituição> deve considerar os diferentes tipos de ativos de hardware de TI que podem estar dentro do escopo da autoavaliação, tais como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem (público, híbrido ou privado de serviço, software como serviço, plataforma como serviço e infraestrutura como serviço etc.)

• Ativos móveis

• Ativos de campo

• Ativos conectados por diferentes redes ou tecnologias de comunicação (por exemplo, modem telefônico, celular)

• Ativos de rede e comunicações

• Recursos de backup, sobressalentes e redundantes, incluindo ativos virtualizados inativos

• Ativos não operacionais, ativos em reparo, ativos em manutenção

• Ativos dependentes de infraestrutura específica, como redes sem fio, serviços de navegação e temporização de posicionamento, e o Sistema de Posicionamento Global (GPS)

• Ativos que podem ser considerados parte da Internet das Coisas ou da Internet das Coisas Industrial

• Ativos que têm potencial para não serem rastreados, não reclamados ou de outra forma negligenciados, como ativos legados, equipamentos de comunicação e ativos que suportam múltiplos grupos

Um inventário não implica que uma única lista seja necessária; múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, a <Instituição> deve, entretanto, considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios.

Um bom inventário de hardware deve conter informações como:

1. Identificação e Rastreamento

Informações que permitem diferenciar um equipamento de outro inequivocamente.

• Hostname (Nome do Dispositivo): O nome de rede do equipamento.

• Número de Série (Serial Number): O identificador único de fábrica (crucial para garantias).

• Etiqueta de Patrimônio: O número de controle interno da sua empresa (aquela etiqueta colada fisicamente).

• Endereço MAC: A "impressão digital" da placa de rede. Essencial para rastreio em logs de DHCP ou Firewall.

• Endereço IP: O endereço lógico atual (se for estático, é ainda mais importante registrar).

2. Especificações Técnicas (Capacidade)

Informações necessárias para o planejamento de upgrades e suporte técnico.

• Fabricante e Modelo: (Ex: Dell Latitude 5420).

• Processador (CPU): Tipo e velocidade.

• Memória RAM: Quantidade total instalada.

• Armazenamento (Disco): Tipo (SSD/HDD) e capacidade total.

• Sistema Operacional e Versão: (Ex: Windows 10 Pro 22H2).

• BIOS/Firmware: Versão atual (crítico para corrigir vulnerabilidades de segurança de baixo nível).

3. Interfaces e Interdependências

Informações necessárias para o planejamento de upgrades e substituições.

• Nome/identificador único da interface que identifique a conexão.

• Tipo de interface (natureza da conexão).

• Identificação dos ativos conectados: ativo(s) fonte/cliente; ativo(s) destino/servidor.

• Propósito da interface

• Criticidade/nível de dependência

• Protocolo(s) e porta(s) utilizado(s)

• Direção do tráfego: inbound, outbound ou bidirecional

4. Localização e Propriedade (Responsabilidade)

Informações fundamentais para auditorias físicas e recuperação de equipamentos.

• Responsável: Quem utiliza o equipamento primariamente.

• Departamento/Centro de Custo: Quem paga pelo equipamento.

• Localização Física: Escritório, Andar, Sala ou, no caso de trabalho remoto, a cidade/estado do colaborador.

• Status do Ativo: Em uso, Em estoque (Disponível), Em manutenção, Aposentado/Descarte.

5. Ciclo de Vida e Financeiro (Gestão)

Informações que ajudam a evitar renovações desnecessárias ou perda de prazos de garantia ou suporte.

• Data de Compra: Para cálculo de depreciação.

• Data de Expiração da Garantia: Para saber se o conserto é custo zero ou pago.

• Fornecedor (Vendor): De quem foi comprado (para acionar suporte).

• Valor de Aquisição: Custo original.

• Data de Fim de Vida (EOL - End of Life): Quando o fabricante parará de dar suporte ou atualizações.

E01-ATIVOS-TI-01-B

O inventário de ativos de hardware de TI inclui ativos dentro da <Instituição> que podem ser alavancados para alcançar um objetivo de ameaça

Detalhamento:

Ativos dentro da <Instituição> são aqueles que a <Instituição> considera como o alvo potencial das táticas ou objetivos de um agente de ameaças. Ao considerar ativos que deveriam receber essa designação, é útil considerar ativos que um agente de ameaças poderia usar para alcançar seu objetivo final, como:

• Ativos voltados para o público que podem servir como ponto de acesso inicial

• Ativos individuais que permitiriam movimento lateral dentro da rede da <Instituição>

• Ativos com direitos administrativos que possibilitariam a escalada de privilégios

Note que a identificação desse conjunto de ativos deve ser baseada em uma avaliação de risco e pode ser informada pelo entendimento da exposição da <Instituição> a ameaças e vulnerabilidades, na medida em que estas sejam conhecidas.

E01-ATIVOS-TI-01-C

Ativos de hardware de TI inventariados são priorizados com base em critérios definidos que incluem importância para a entrega da <Instituição>

Detalhamento:

A priorização dos ativos é importante para muitas atividades operacionais e de cibersegurança, como resposta a incidentes, gestão de riscos, gestão de ameaças e planejamento da arquitetura de cibersegurança. Existem múltiplas abordagens para priorização de ativos: classificação forçada (lista sequencial), classificação em níveis (por exemplo, todos os ativos lidando com o fluxo de gás são de nível 1, ativos relacionados à eficiência e monitoramento são de nível 2, e funções não críticas como relações públicas e marketing são de nível 3). Os níveis devem ser baseados em critérios definidos, como importância do ativo para a <Instituição> (por exemplo, segurança, criticidade do ativo para a entrega da <Instituição>, escassez do ativo, quão dependentes outros ativos são desse ativo) ou a sensibilidade dos dados armazenados ou processados pelo ativo. As prioridades devem ser documentadas e, idealmente, acordadas por todas as partes interessadas envolvidas. Elas também devem ser comunicadas em toda a <Instituição> para uso em resposta a incidentes, gestão de riscos e outras atividades relevantes. Por exemplo, ativos virtualizados podem apresentar risco aumentado devido a questões como expansão dos ativos e suas características únicas (facilidade de captura de instantâneos e armazenamento de máquinas virtuais dormentes como arquivos) e, portanto, podem representar maior risco para a <Instituição>. Qualquer que seja a abordagem utilizada, a importância do ativo para a entrega da <Instituição> deve ser um dos critérios de priorização utilizados.

E01-ATIVOS-TI-01-D

Os critérios de priorização incluem a consideração do grau em que um ativo dentro da <Instituição> pode ser aproveitado para alcançar um objetivo de ameaça

Detalhamento:

A possibilidade de um ativo ser alavancado para alcançar um objetivo de ameaça é adicionada aos critérios para priorizar ativos de hardware de TI. É importante considerar que um agente de ameaças pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes situações. Incluir critérios adicionais além daqueles usados para ativos importantes para a execução da <Instituição> permitirá uma priorização mais abrangente dos riscos e impactos associados aos ativos de hardware de TI.

E01-ATIVOS-TI-01-E

O inventário de ativos de hardware de TI inclui atributos que suportam atividades de cibersegurança (por exemplo, localização, prioridade de ativos, proprietário do ativo, sistema operacional e versões de firmware)

Detalhamento:

Atributos de inventário são detalhes sobre ativos incluídos nos inventários de ativos para permitir a gestão e o uso consistente dos ativos. Incluir informações necessárias sobre ativos para apoiar as atividades do programa de cibersegurança ajuda a garantir que essas informações estejam disponíveis durante períodos de estresse operacional e não precisem ser coletadas em estado de crise. Por exemplo, os respondentes de incidentes poderão identificar facilmente a prioridade, criticidade e localização das máquinas que são afetadas por um evento de bloqueio e precisam ser substituídas.

Além disso, atributos de inventário podem ser usados para indicar aspectos de ativos que podem exigir atenção ou tratamento especial, como sistemas que utilizam inteligência artificial ou aprendizado de máquina. Exemplos de atributos potenciais de inventário incluem localizações físicas, localizações de rede, importância para a entrega da <Instituição>, impacto em caso de violação, datas de fim de vida, datas de fim de suporte, sistema operacional, firmware, versões.

E01-ATIVOS-TI-01-F

O inventário de ativos de hardware de TI está completo (o inventário inclui todos os ativos da <Instituição>)

Detalhamento:

Esta <Ação> amplia o escopo do inventário. Qualquer ativo de TI relacionado à entrega da <Instituição> deve ser identificado e inventariado, junto com seus atributos. A relação entre ativos e funções empresariais também deve ser incluída para permitir a priorização e o desenvolvimento de estratégias de proteção e sustentação. A implementação do inventário deve ser proporcional ao tamanho, complexidade e risco da <Instituição>. Por exemplo, para uma empresa pequena e de baixa complexidade, uma planilha simples pode ser usada para o estoque. Para empresas maiores e mais complexas, métodos mais sofisticados, como a aplicação dedicada de inventário de ativos, são apropriados. a <Instituição> pode considerar implementar ferramentas para identificar quais dispositivos estão conectados às redes e identificar novas conexões inesperadas.

a <Instituição> deve considerar os diferentes tipos de ativos de hardware de TI que podem estar dentro do escopo da autoavaliação, tais como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem (público, híbrido ou privado de serviço, software como serviço, plataforma como serviço e infraestrutura como serviço etc.)

• Ativos móveis

• Ativos de campo

• Ativos de backup, sobressalentes e redundantes, incluindo ativos virtualizados inativos

• Ativos dependentes de infraestrutura específica como redes sem fio, serviços de navegação e temporização de posicionamento, e os ativos do Sistema de Posição Global que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas

Inventário refere-se a uma listagem completa e não pretende implicar que uma única lista seja necessária; Múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, entretanto, a <Instituição> deve considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios. As tecnologias de descoberta de ativos estão aumentando em capacidade e disponibilidade e podem ser aproveitadas para realizar esta <Ação>.

E01-ATIVOS-TI-01-G

O inventário de ativos de hardware de TI é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema

Detalhamento:

O inventário de ativos e componentes significativos deve ser atualizado e mantido conforme os ativos mudam ao longo de seu ciclo de vida para garantir que o inventário seja completo e preciso. Garantir que o estoque de ativos esteja atualizado pode envolver procedimentos de gerenciamento de mudanças que exigem atualizações de estoque sempre que os ativos são trocados ou significativamente alterados.

a <Instituição> também pode realizar revisões de estoque, tanto periodicamente (como trimestral ou anualmente) quanto com base em eventos (como mudanças na estrutura organizacional, grandes mudanças na infraestrutura tecnológica e aquisição e consolidação de outro negócio). a <Instituição> pode considerar implementar ferramentas que possibilitem a descoberta automatizada de ativos e forneçam uma compreensão mais em tempo real dos inventários.

E01-ATIVOS-TI-02

Gerenciar a configuração de ativos de hardware de TI

E01-ATIVOS-TI-02-A

As linhas de base de configuração do hardware de TI são estabelecidas

Detalhamento:

Estabelecer uma linha de base para ativos de hardware de TI fornece uma base para gerenciar a integridade dos ativos à medida que mudam ao longo de seu ciclo de vida. Estabelecer capturas pontuais-in-tempo dos ativos (itens de configuração) garante que esses ativos possam ser restaurados a uma forma aceitável quando necessário — após uma interrupção, quando ocorreu uma modificação não autorizada ou em qualquer circunstância em que a integridade seja duvidosa e forneça um nível de controle sobre mudanças que possam potencialmente prejudicar o suporte dos ativos aos serviços organizacionais.

a <Instituição> pode considerar mecanismos de verificação de integridade (manual ou automática) ao realizar capturas pontuais-in-tempo de ativos e configurações de ativos. O uso de mecanismos de verificação de integridade para verificar capturas em um momento específico antes da restauração pode ajudar a garantir que elas sejam viáveis e disponíveis.

Políticas e procedimentos documentados para a configuração ou manutenção de linhas de base não são obrigatórios para implementar esta <Ação>.

E01-ATIVOS-TI-02-B

As linhas de base de configuração são usadas para configurar ativos de hardware de TI na implantação e restauração

Detalhamento:

A <Instituição> possui procedimentos para garantir que linhas de base de configuração estabelecidas sejam aplicadas aos ativos quando eles são implantados e restaurados. Essas linhas de base (também chamadas de builds padrão) suportam o deslocamento de ativos de forma controlada.

E01-ATIVOS-TI-02-C

As linhas de base de configuração incorporam os requisitos aplicáveis da arquitetura de cibersegurança

Detalhamento:

Como parte da arquitetura de cibersegurança, a <Instituição> seleciona e documenta os requisitos para o nível adequado de confidencialidade, integridade e disponibilidade de ativos de hardware de TI. Esses requisitos podem então ser usados para impulsionar o desenvolvimento de controles de cibersegurança a serem aplicados a ativos e sistemas (como linhas de base de configuração, proteções de rede, segurança de software). Diretrizes de reforço da linha de base de configuração, como os Center for Internet Security Benchmarks ou os Guias Técnicos de Implementação de Segurança (STIGs) do

Departamento de Defesa, podem fornecer um ponto de partida para selecionar configurações que atendam aos requisitos da arquitetura de cibersegurança.

E01-ATIVOS-TI-02-D

As linhas de base de configuração são revisadas e atualizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e alterações na arquitetura de cibersegurança

Detalhamento:

A <Instituição> possui um cronograma definido para revisar regularmente as linhas de base e atualizá-las conforme necessário, garantindo que continuem refletindo requisitos adequados de segurança e funcionalidade.

E01-ATIVOS-TI-02-E

As configurações dos ativos são monitoradas para garantir consistência com as linhas de base ao longo dos ciclos de vida dos ativos

Detalhamento:

a <Instituição> deve monitorar as configurações dos ativos para garantir que continuem a se conformar às linhas de base ao longo do tempo após a implantação. O monitoramento de consistência pode ser feito por meios automatizados, como o uso de uma ferramenta de varredura que compare as linhas de base dos ativos conectados com as linhas de configuração estabelecidas, ou realizando auditorias periódicas dos ativos para determinar se mudanças não autorizadas foram feitas. Ferramentas também podem ser usadas para reverter automaticamente os ativos para referências.

Ferramentas automatizadas de gerenciamento de configuração ou monitoramento podem permitir um rastreamento mais eficiente das configurações dos ativos. Ferramentas capazes de abranger ambientes físicos, virtuais, móveis, híbridos e outros ambientes tecnológicos devem ser consideradas para ajudar a garantir cobertura adequada dos ativos de hardware de TI. Essas ferramentas podem ser otimizadas para produtos específicos. Ao selecionar ferramentas de automação, os stakeholders com treinamento e experiência adequados devem ser engajados desde cedo e deve ser dada uma consideração cuidadosa para garantir a adequação adequada entre as ferramentas de automação e os produtos com os quais elas se destinam a integrar.

Ferramentas de integridade de dados (como checksums criptográficos) podem ajudar na detecção de alterações não autorizadas nas configurações de configuração, especialmente ao gerenciar ativos virtualizados. Como exemplo disso, uma <Instituição> pode implementar verificações de integridade de arquivos para plataformas de virtualização a serem realizadas na inicialização e confirmar que nenhuma alteração não autorizada ocorreu.

E01-ATIVOS-TI-03

Gerenciar alterações nos ativos de hardware de TI

E01-ATIVOS-TI-03-A

Mudanças nos ativos são avaliadas e aprovadas antes de serem implementadas

Detalhamento:

Todas as mudanças propostas nos ativos inventariados são avaliadas para entender sua prioridade, benefícios, riscos e impactos na funcionalidade e segurança das funções que suportam. Considere que eles podem variar entre diferentes tipos de ativos de hardware de TI, como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem

• Ativos móveis

• Ativos de campo

• Ativos dependentes de infraestrutura específica como redes sem fio ou o Sistema Global de Posição

• Ativos que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas.

E01-ATIVOS-TI-03-B

Mudanças nos ativos são documentadas

Detalhamento:

Quaisquer alterações feitas em um ativo inventariado são capturadas em um formato que pode ser facilmente referenciado durante atividades de resolução de problemas ou resposta a incidentes. As mudanças podem incluir a alteração de configurações como roteamento e configurações de portas em dispositivos de rede, a adição ou remoção de componentes e a modificação de privilégios de acesso. Alguns dos atributos que devem ser registrados incluem data e hora da mudança, o responsável pela alteração, os ativos afetados pela mudança e uma descrição de quaisquer riscos associados à mudança.

E01-ATIVOS-TI-03-C

Os requisitos de documentação para alterações de ativos são estabelecidos e mantidos

Detalhamento:

A <Instituição> deve definir as informações necessárias que devem ser documentadas ao realizar mudanças nos ativos de hardware de TI. Os requisitos devem considerar informações que podem ser necessárias para atividades como solução de problemas ou resposta a incidentes.

Além disso, a <Instituição> deve considerar a manutenção desses requisitos com base nas mudanças no ambiente operacional.

E01-ATIVOS-TI-03-D

Mudanças em ativos de prioridade mais alta são testadas antes de serem implantadas

Detalhamento:

Mudanças nos ativos devem ser testadas para garantir a continuidade desses ativos e funções afetadas antes de se implementar as mudanças em toda a <Instituição>. Quando possível, os testes das mudanças propostas devem ser realizados em um ambiente de teste ou em um ambiente de produção de baixo risco. Os testes podem incluir testes de estresse, confirmação de que mudanças foram implementadas, operabilidade e testes de carga.

Além disso, a <Instituição> pode considerar se controles que impedem mudanças não autorizadas são necessários para tipos específicos de ativos. Por exemplo, interruptores de programação digitais ou de

hardware devem ser colocados em um modo que não permita programação durante operações rotineiras.

E01-ATIVOS-TI-03-E

Mudanças e atualizações são implementadas de forma segura

Detalhamento:

Procedimentos e ferramentas usados para atualizar ativos devem incorporar controles apropriados para garantir que vulnerabilidades ou configurações incorretas ou não intencionais sejam introduzidas como parte dos processos de mudança de ativos. Isso pode incluir o uso de protocolos de comunicação segura, métodos de verificação, como assinaturas digitais, ou outros controles.

E01-ATIVOS-TI-03-F

A capacidade de reverter mudanças é estabelecida e mantida para ativos importantes para a execução da <Instituição>

Detalhamento:

Esta <Ação> descreve o desenvolvimento da capacidade de reverter mudanças após sua aplicação. Isso pode ser alcançado por métodos manuais ou automatizados. Isso permite que uma <Instituição> volte a um estado conhecido caso uma mudança crie consequências operacionais ou de segurança imprevistas ou não intencionais que não possam ser resolvidas por outros meios.

E01-ATIVOS-TI-03-G

As <Ações> de gestão de mudanças abrangem todo o ciclo de vida dos ativos (por exemplo, aquisição, implantação, operação, aposentadoria)

Detalhamento:

As condições organizacionais e operacionais estão em constante mudança, resultando em mudanças na equipe, no conteúdo e uso dos dados, na tecnologia, entre outros. Essas mudanças podem impactar ativos importantes ao longo de seus ciclos de vida. As <Ações> de gestão de mudanças não devem se limitar a mudanças nos ativos operacionalmente implantados, mas devem abranger todas as fases do ciclo de vida, incluindo aquisição, implantação e aposentadoria.

Para isso, a <Instituição> deve definir e gerenciar o processo para manter o inventário de ativos atualizado e garantir que mudanças no estoque não resultem em lacunas nas estratégias para proteger e manter os ativos.

Além disso, a <Instituição> deve monitorar ativamente mudanças que alterem significativamente os ativos, identificar novos ativos e pedir a aposentadoria de ativos para os quais não haja mais necessidade ou cujo valor relativo tenha sido reduzido.

Considere que diferentes tipos de tecnologias (como ativos virtualizados e ativos em nuvem) podem ter estágios únicos do ciclo de vida e outros aspectos distintos que impactam como a gestão de mudanças deve ser implementada.

E01-ATIVOS-TI-03-H

Mudanças em ativos de prioridade mais alta são testadas quanto ao impacto em cibersegurança antes de serem implantadas

Detalhamento:

Alterações em um ativo usado em múltiplos serviços podem atender a uma necessidade imediata, mas causar problemas em outras aplicações. As mudanças devem ser avaliadas em um ambiente de teste para identificar qualquer impacto da mudança proposta em outros ativos e sistemas. O impacto na cibersegurança pode incluir qualquer impacto na disponibilidade de um ativo para usuários autorizados, enfraquecimento das proteções ou alterações não intencionais nas listas de controle de acesso. Por exemplo, se um fornecedor lança uma nova versão de um sistema operacional, o novo sistema operacional deve ser testado em um ambiente controlado para determinar se algum aplicativo ou serviço seria afetado.

E01-ATIVOS-TI-03-I

Os registros de alterações incluem informações sobre modificações que impactam os requisitos de cibersegurança dos ativos

Detalhamento:

Se testes de impacto em cibersegurança antes da implantação de alterações nos ativos revelarem que os requisitos de cibersegurança (confidencialidade, integridade, autenticidade e disponibilidade) serão afetados, esses impactos devem ser descritos nos registros de alterações quando os ativos forem alterados. Por exemplo, se os esquemas de endereçamento IP forem alterados dentro de um dispositivo de rede, o registro de alterações deve indicar como a disponibilidade de dispositivos conectados pode ser afetada.

E01-ATIVOS-TI-04

Gerenciar inventário de ativos de software de TI

E01-ATIVOS-TI-04-A

Os ativos de software de TI importantes para a entrega da <Instituição> são inventariados

Detalhamento:

Os ativos obtêm seu valor e importância por meio de sua associação com os aspectos das operações da <Instituição> que suportam. Identificar e inventariar ativos de software de TI de alto valor ajuda a possibilitar a seleção e aplicação de controles apropriados. a <Instituição> deve considerar os diferentes tipos de ativos de software de TI que podem estar dentro do escopo da autoavaliação, coletando dados relevantes sobre o software, pois um inventário de software eficiente vai muito além de uma simples lista de nomes. Ele precisa fornecer contexto para segurança, licenciamento e suporte.

Aqui estão os elementos comuns e essenciais divididos por categorias:

1. Identificação Básica do Software: estes dados respondem "o que é isso?" e "quem o fez?".

• Nome do Software: Nome completo e comercial (ex: TIA Portal, Windows Server 2022).

• Versão e Build: Crucial para identificar se o software está atualizado ou vulnerável.

• Fabricante (Vendor): Quem fornece o suporte e as atualizações (ex: Siemens, Microsoft, Oracle).

• ID do Ativo (Tag): Um identificador único que vincula o software a um registro no banco de dados de ativos.

2. Contexto de Instalação e Localização: estes dados respondem "onde ele está rodando?".

• Hostname/Dispositivo: Nome do servidor, workstation ou PLC onde o software reside.

• Caminho de Instalação (Path): Localização no diretório do sistema (importante para detectar executáveis maliciosos).

• Ambiente: Se o software está em Produção, Homologação ou Desenvolvimento.

• Tipo de Instalação: Se é local, SaaS (nuvem), máquina virtual ou container.

3. Gestão de Segurança e Vulnerabilidades: estes dados são essenciais para os <Eixos> AMEAÇAS e CONFIGURAÇÃO.

• Status de Suporte (EOL/EOS): Indica se o software já chegou ao fim da vida útil (End of Life) ou fim do suporte, o que representa um risco crítico.

• CVEs Conhecidas: Lista de vulnerabilidades associadas àquela versão específica.

• Nível de Criticidade: Qual o impacto para o negócio se esse software parar ou for invadido?

• Assinatura Digital: Se o executável é assinado e verificado por um fornecedor confiável.

4. Gestão de Licenciamento e Conformidade: estes dados são focados em custos e aspectos legais.

• Tipo de Licença: (SaaS, Perpétua, Open Source, Freeware).

• Data de Expiração: quando a licença ou o contrato de manutenção precisa ser renovado.

• Quantidade de Instalações: quantas instâncias estão em uso vs. quantas foram adquiridas.

• Requisitos de Atualização (Patch): se o software aceita atualizações automáticas ou exige intervenção manual (janela de manutenção).

==========

Elementos Específicos para Software de TO (Tecnologia Operacional)

Ativos de TO demandam informações particularidades:

• Versão do Firmware: para controladores (PLCs) o firmware é o "software" principal.

• Protocolos de Comunicação: quais protocolos o software utiliza (Modbus, Profinet, etc).

• Dependência de Hardware: se o software demanda uma versão específica de hardware proprietário.

• Dependência de Software: se o software demanda uma versão específica de software (proprietário ou comercial).

==========

É importante atentar para ativos que têm potencial para não serem rastreados, não reclamados ou de outra forma negligenciados, como ativos legados, equipamentos de comunicação e ativos que suportam múltiplos grupos

Um inventário não implica que uma única lista seja necessária; múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, a <Instituição> deve, entretanto, considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios.

E01-ATIVOS-TI-04-B

O inventário de ativos de software de TI inclui ativos dentro da <Instituição> que podem ser alavancados para alcançar um objetivo de ameaça

Detalhamento:

Ativos dentro da <Instituição> são aqueles que a <Instituição> considera como o alvo potencial das táticas ou objetivos de um agente de ameaças. Ao considerar ativos que deveriam receber essa designação, é útil considerar ativos que um agente de ameaças poderia usar para alcançar seu objetivo final, como:

• Ativos voltados para o público que podem servir como ponto de acesso inicial

• Ativos individuais que permitiriam movimento lateral dentro da rede da <Instituição>

• Ativos com direitos administrativos que possibilitariam a escalada de privilégios

Note que a identificação desse conjunto de ativos deve ser baseada em uma avaliação de risco e pode ser informada pelo entendimento da exposição da <Instituição> a ameaças e vulnerabilidades, na medida em que estas sejam conhecidas.

E01-ATIVOS-TI-04-C

Ativos de software de TI inventariados são priorizados com base em critérios definidos que incluem importância para a entrega da <Instituição>

Detalhamento:

A priorização dos ativos é importante para muitas atividades operacionais e de cibersegurança, como resposta a incidentes, gestão de riscos, gestão de ameaças e planejamento da arquitetura de cibersegurança. Existem múltiplas abordagens para priorização de ativos: classificação forçada (lista sequencial), classificação em níveis (por exemplo, todos os ativos lidando com o fluxo de gás são de nível 1, ativos relacionados à eficiência e monitoramento são de nível 2, e funções não críticas como relações públicas e marketing são de nível 3). Os níveis devem ser baseados em critérios definidos, como importância do ativo para a <Instituição> (por exemplo, segurança, criticidade do ativo para a entrega da <Instituição>, escassez do ativo, quão dependentes outros ativos são desse ativo) ou a sensibilidade dos dados armazenados ou processados pelo ativo. As prioridades devem ser documentadas e, idealmente, acordadas por todas as partes interessadas envolvidas. Eles também devem ser comunicados em toda a <Instituição> para uso em resposta a incidentes, gestão de riscos e outras atividades relevantes. Por exemplo, ativos virtualizados podem apresentar risco aumentado devido a questões como expansão dos ativos e suas características únicas (facilidade de captura de instantâneos e armazenamento de máquinas virtuais dormentes como arquivos) e, portanto, podem representar maior risco para a <Instituição>. Qualquer que seja a abordagem utilizada, a importância do ativo para a entrega da <Instituição> deve ser um dos critérios de priorização utilizados.

E01-ATIVOS-TI-04-D

Os critérios de priorização incluem a consideração do grau em que um ativo dentro da <Instituição> pode ser aproveitado para alcançar um objetivo de ameaça

Detalhamento:

A possibilidade de um ativo ser alavancado para alcançar um objetivo de ameaça é adicionada aos critérios para priorizar ativos de software de TI. É importante considerar que um agente de ameaças pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes

situações. Incluir critérios adicionais além daqueles usados para ativos importantes para a execução da <Instituição> permitirá uma priorização mais abrangente dos riscos e impactos associados aos ativos de software de TI.

E01-ATIVOS-TI-04-E

O inventário de ativos de software de TI inclui atributos que suportam atividades de cibersegurança (por exemplo, localização, prioridade do ativo, proprietário do ativo, e versões de bibliotecas)

Detalhamento:

Atributos de inventário são detalhes sobre ativos incluídos nos inventários de ativos para permitir a gestão e o uso consistente dos ativos. Incluir informações necessárias sobre ativos para apoiar as atividades do programa de cibersegurança ajuda a garantir que essas informações estejam disponíveis durante períodos de estresse operacional e não precisem ser coletadas em estado de crise. Por exemplo, os respondentes de incidentes poderão identificar facilmente a prioridade, criticidade e localização das máquinas que são afetadas por um evento de bloqueio e precisam ser substituídas.

Além disso, atributos de inventário podem ser usados para indicar aspectos de ativos que podem exigir atenção ou tratamento especial, como sistemas que utilizam inteligência artificial ou aprendizado de máquina. Exemplos de atributos potenciais de inventário incluem localizações físicas, localizações de rede, importância para a entrega da <Instituição>, impacto em caso de violação, datas de fim de vida, datas de fim de suporte, sistema operacional, firmware, versões.

E01-ATIVOS-TI-04-F

O inventário de ativos de software de TI está completo (o inventário inclui todos os ativos da <Instituição>)

Detalhamento:

Esta <Ação> amplia o escopo do inventário. Qualquer ativo de software de TI relacionado à entrega da <Instituição> deve ser identificado e inventariado, junto com seus atributos. A relação entre ativos e funções empresariais também deve ser incluída para permitir a priorização e o desenvolvimento de estratégias de proteção e sustentação. A implementação do inventário deve ser proporcional ao tamanho, complexidade e risco da <Instituição>. Por exemplo, para uma empresa pequena e de baixa complexidade, uma planilha simples pode ser usada para o estoque. Para empresas maiores e mais complexas, métodos mais sofisticados, como a aplicação dedicada de inventário de ativos, são apropriados. a <Instituição> pode considerar implementar ferramentas para identificar quais dispositivos estão conectados às redes e identificar novas conexões inesperadas.

a <Instituição> deve considerar os diferentes tipos de ativos de software de TI que podem estar dentro do escopo da autoavaliação, tais como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem (público, híbrido ou privado de serviço, software como serviço, plataforma como serviço e infraestrutura como serviço etc.)

• Ativos móveis

• Ativos de campo

• Ativos de backup, sobressalentes e redundantes, incluindo ativos virtualizados inativos

• Ativos dependentes de infraestrutura específica como redes sem fio, serviços de navegação e temporização de posicionamento, e os ativos do Sistema de Posição Global que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas

Inventário refere-se a uma listagem completa e não pretende implicar que uma única lista seja necessária; Múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, entretanto, a <Instituição> deve considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios. As tecnologias de descoberta de ativos estão aumentando em capacidade e disponibilidade e podem ser aproveitadas para realizar esta <Ação>.

E01-ATIVOS-TI-04-G

O inventário de ativos de software de TI está atualizado, ou seja, é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema

Detalhamento:

O inventário de ativos e componentes significativos deve ser atualizado e mantido conforme os ativos mudam ao longo de seu ciclo de vida para garantir que o inventário seja completo e preciso. Garantir que o estoque de ativos esteja atualizado pode envolver procedimentos de gerenciamento de mudanças que exigem atualizações de estoque sempre que os ativos são trocados ou significativamente alterados. a <Instituição> também pode realizar revisões de estoque, tanto periodicamente (como trimestral ou anualmente) quanto com base em eventos (como mudanças na estrutura organizacional, grandes mudanças na infraestrutura tecnológica e aquisição e consolidação de outro negócio). a <Instituição> pode considerar implementar ferramentas que possibilitem a descoberta automatizada de ativos e forneçam uma compreensão mais em tempo real dos inventários.

E01-ATIVOS-TI-05

Gerenciar a configuração de ativos de software de TI

E01-ATIVOS-TI-05-A

As linhas de base de configuração são estabelecidas

Detalhamento:

Estabelecer uma linha de base para ativos de software de TI fornece uma base para gerenciar a integridade dos ativos à medida que mudam ao longo de seu ciclo de vida. Estabelecer capturas pontuais-no-tempo dos ativos (itens de configuração) garante que esses ativos possam ser restaurados a uma forma aceitável quando necessário — após uma interrupção, quando ocorreu uma modificação não autorizada ou em qualquer circunstância em que a integridade seja duvidosa e forneça um nível de controle sobre mudanças que possam potencialmente prejudicar o suporte dos ativos aos serviços organizacionais.

a <Instituição> pode considerar mecanismos de verificação de integridade (manual ou automática) ao realizar capturas pontuais-no-tempo de ativos e configurações de ativos. O uso de mecanismos de verificação de integridade para verificar capturas em um momento específico antes da restauração pode ajudar a garantir que elas sejam viáveis e disponíveis.

Políticas e procedimentos documentados para a configuração ou manutenção de linhas de base não são obrigatórios para implementar esta <Ação>.

E01-ATIVOS-TI-05-B

Linhas de base de configuração são usadas para configurar ativos na implantação e restauração

Detalhamento:

A <Instituição> possui procedimentos para garantir que linhas de base de configuração estabelecidas sejam aplicadas aos ativos quando eles são implantados e restaurados. Essas linhas de base (também chamadas de builds padrão) suportam o deslocamento de ativos de forma controlada.

E01-ATIVOS-TI-05-C

As linhas de base de configuração incorporam os requisitos aplicáveis da arquitetura de cibersegurança

Detalhamento:

Como parte da arquitetura de cibersegurança, a <Instituição> seleciona e documenta os requisitos para o nível adequado de confidencialidade, integridade e disponibilidade de ativos de software de TI. Esses requisitos podem então ser usados para impulsionar o desenvolvimento de controles de cibersegurança a serem aplicados a ativos e sistemas (como linhas de base de configuração, proteções de rede, segurança de software). Diretrizes de reforço da linha de base de configuração podem fornecer um ponto de partida para selecionar configurações que atendam aos requisitos da arquitetura de cibersegurança.

E01-ATIVOS-TI-05-D

As linhas de base de configuração são revisadas e atualizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e alterações na arquitetura de cibersegurança

Detalhamento:

A <Instituição> possui um cronograma definido para revisar regularmente as linhas de base e atualizá-las conforme necessário, garantindo que continuem refletindo requisitos adequados de segurança e funcionalidade.

E01-ATIVOS-TI-05-E

As configurações dos ativos são monitoradas para garantir consistência com as linhas de base ao longo dos ciclos de vida dos ativos

Detalhamento:

a <Instituição> deve monitorar as configurações dos ativos para garantir que continuem a se conformar às linhas de base ao longo do tempo após a implantação. O monitoramento de consistência pode ser feito por meios automatizados, como o uso de uma ferramenta de varredura que compare as linhas de base dos ativos conectados com as linhas de configuração estabelecidas, ou realizando auditorias periódicas dos ativos para determinar se mudanças não autorizadas foram feitas. Ferramentas também podem ser usadas para reverter automaticamente os ativos para referências.

Ferramentas automatizadas de gerenciamento de configuração ou monitoramento podem permitir um rastreamento mais eficiente das configurações dos ativos. Ferramentas capazes de abranger ambientes físicos, virtuais, móveis, híbridos e outros ambientes tecnológicos devem ser consideradas para ajudar a garantir cobertura adequada dos ativos de software de TI. Essas ferramentas podem ser otimizadas para produtos específicos. Ao selecionar ferramentas de automação, os stakeholders com treinamento

e experiência adequados devem ser engajados desde cedo e deve ser dada uma consideração cuidadosa para garantir a adequação adequada entre as ferramentas de automação e os produtos com os quais elas se destinam a integrar.

Ferramentas de integridade de dados (como checksums criptográficos) podem ajudar na detecção de alterações não autorizadas nas configurações de configuração, especialmente ao gerenciar ativos virtualizados. Como exemplo disso, uma <Instituição> pode implementar verificações de integridade de arquivos para plataformas de virtualização a serem realizadas na inicialização e confirmar que nenhuma alteração não autorizada ocorreu.

E01-ATIVOS-TI-06

Gerenciar alterações nos ativos de software de TI

E01-ATIVOS-TI-06-A

Mudanças nos ativos são avaliadas e aprovadas antes de serem implementadas

Detalhamento:

Todas as mudanças propostas nos ativos inventariados são avaliadas para entender sua prioridade, benefícios, riscos e impactos na funcionalidade e segurança das funções que suportam. Considere que eles podem variar entre diferentes tipos de ativos de TO, TO e de informação, como:

- Ativos virtualizados
- Ativos regulados
- Ativos gerenciados por terceiros
- Ativos BYOD
- Ativos em nuvem
- Ativos móveis
- Ativos de campo
- Ativos dependentes de infraestrutura específica como redes sem fio ou o Sistema Global de Posição
- Ativos que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas.

E01-ATIVOS-TI-06-B

Mudanças nos ativos são documentadas

Detalhamento:

Quaisquer alterações feitas em um ativo inventariado são capturadas em um formato que pode ser facilmente referenciado durante atividades de resolução de problemas ou resposta a incidentes. As mudanças podem incluir a alteração de configurações como roteamento e configurações de portas em dispositivos de rede, a adição ou remoção de componentes e a modificação de privilégios de acesso. Alguns dos atributos que devem ser registrados incluem data e hora da mudança, quem fez a alteração, os ativos afetados pela mudança e uma descrição de quaisquer riscos associados à mudança.

E01-ATIVOS-TI-06-C

Os requisitos de documentação para alterações de ativos são estabelecidos e mantidos

Detalhamento:

A <Instituição> deve definir as informações necessárias que devem ser documentadas ao realizar mudanças nos ativos de TO. Os requisitos devem considerar quais informações podem ser necessárias para atividades como solução de problemas ou resposta a incidentes.

Além disso, a <Instituição> deve considerar a manutenção desses requisitos com base nas mudanças no ambiente operacional.

E01-ATIVOS-TI-06-D

Mudanças em ativos de prioridade mais alta são testadas antes de serem implantadas

Detalhamento:

Mudanças nos ativos devem ser testadas para garantir a continuidade dos ativos e funções que afetam antes de implementar as mudanças em toda a empresa. Quando possível, os testes das mudanças propostas devem ser realizados em um ambiente de teste ou em um ambiente de produção de baixo risco. Os testes podem incluir testes de estresse, confirmação de que mudanças foram implementadas, operabilidade e testes de carga.

Além disso, a <Instituição> pode considerar se controles que impedem mudanças não autorizadas são necessários para tipos específicos de ativos. Por exemplo, interruptores de programação digitais ou de hardware devem ser colocados em um modo que não permita programação durante operações rotineiras.

E01-ATIVOS-TI-06-E

Mudanças e atualizações são implementadas de forma segura

Detalhamento:

Procedimentos e ferramentas usados para atualizar ativos devem incorporar controles apropriados para garantir que vulnerabilidades ou configurações incorretas ou não intencionais sejam introduzidas como parte dos processos de mudança de ativos. Isso pode incluir o uso de protocolos de comunicação segura, métodos de verificação, como assinaturas digitais, ou outros controles.

E01-ATIVOS-TI-06-F

A capacidade de reverter mudanças é estabelecida e mantida para ativos importantes para a execução da <Instituição>

Detalhamento:

Esta <Ação> descreve o desenvolvimento da capacidade de reverter mudanças após sua aplicação. Isso pode ser alcançado por métodos manuais ou automatizados. Isso permite que uma <Instituição> volte a um estado conhecido de bom caso uma mudança crie consequências operacionais ou de segurança imprevistas ou não intencionais que não possam ser resolvidas por outros meios.

E01-ATIVOS-TI-06-G

As <Ações> de gestão de mudanças abrangem todo o ciclo de vida dos ativos (por exemplo, aquisição, implantação, operação, aposentadoria)

Detalhamento:

As condições organizacionais e operacionais estão em constante mudança, resultando em mudanças na equipe, no conteúdo e uso dos dados, na tecnologia, entre outros. Essas mudanças podem impactar ativos importantes ao longo de seus ciclos de vida. As <Ações> de gestão de mudanças não devem se limitar a mudanças nos ativos operacionalmente implantados, mas devem abranger todas as fases do ciclo de vida, incluindo aquisição, implantação e aposentadoria.

Para isso, a <Instituição> deve definir e gerenciar o processo para manter o inventário de ativos atualizado e garantir que mudanças no estoque não resultem em lacunas nas estratégias para proteger e manter os ativos.

Além disso, a <Instituição> deve monitorar ativamente mudanças que alterem significativamente os ativos, identificar novos ativos e pedir a aposentadoria de ativos para os quais não há mais necessidade ou cujo valor relativo foi reduzido.

Considere que diferentes tipos de tecnologias (como ativos virtualizados e ativos em nuvem) podem ter estágios únicos do ciclo de vida e outros aspectos distintos que impactam como a gestão de mudanças deve ser implementada.

E01-ATIVOS-TI-06-H

Mudanças em ativos de prioridade mais alta são testadas quanto ao impacto em cibersegurança antes de serem implantadas

Detalhamento:

Alterações em um ativo usado em múltiplos serviços podem atender a uma necessidade imediata, mas causar problemas em outras aplicações. As mudanças devem ser avaliadas em um ambiente de teste para identificar qualquer impacto da mudança proposta em outros ativos e sistemas. O impacto na cibersegurança pode incluir qualquer impacto na disponibilidade de um ativo para usuários autorizados, enfraquecimento das proteções ou alterações não intencionais nas listas de controle de acesso. Por exemplo, se um fornecedor lança uma nova versão de um sistema operacional, o novo sistema operacional deve ser testado em um ambiente controlado para determinar se algum aplicativo ou serviço seria afetado.

E01-ATIVOS-TI-06-I

Os registros de alterações incluem informações sobre modificações que impactam os requisitos de cibersegurança dos ativos

Detalhamento:

Se testes de impacto em cibersegurança antes da implantação de alterações nos ativos revelarem que os requisitos de cibersegurança (confidencialidade, integridade e disponibilidade) serão afetados, esses impactos devem ser descritos nos registros de alterações quando os ativos forem alterados. Por exemplo, se os esquemas de endereçamento IP forem alterados dentro de um dispositivo de rede, o registro de alterações deve indicar como a disponibilidade de dispositivos conectados pode ser afetada.

E02-CIBERFÍSICOS

Gerenciamento de ativos, alterações e configuração

Resumo:

Um ativo é algo de valor para uma <Instituição>. Para os fins do modelo, os ativos a serem considerados são ativos de hardware e software de TO, bem como informações essenciais para operar a função.

Detalhamento:

Um inventário de ativos importantes para a execução da função é um recurso importante na gestão de ciber-riscos. O registro de informações importantes, como versão do software, localização física, proprietário do ativo e prioridade, possibilita muitas outras <Ações> de gestão de cibersegurança. Por exemplo, um inventário de ativos robusto pode identificar o local de implantação do software que requer aplicação de patches.

Gerenciar a configuração de ativos envolve definir uma linha de base de configuração e garantir que os ativos sejam configurados de acordo com essa linha de base. Normalmente, essa prática se aplica para garantir que ativos semelhantes sejam configurados da mesma maneira. No entanto, nos casos em que os ativos são únicos ou devem ter configurações individuais, o gerenciamento da configuração de ativos envolve o controle da linha de base de configuração.

O gerenciamento de alterações nos ativos inclui a análise das alterações solicitadas para garantir que elas não introduzam vulnerabilidades inaceitáveis no ambiente operacional, garantindo que todas as alterações sigam o processo de gerenciamento de alterações e identificando alterações não autorizadas. O controle de alterações se aplica a todo o ciclo de vida do ativo, incluindo definição de requisitos, testes, implantação e manutenção e desativação da operação.

E02-CIBERFÍSICOS-01

Gerenciar o inventário de ativos de hardware de TO

E02-CIBERFÍSICOS-01-A

Os ativos de TO importantes para a entrega da <Instituição> são inventariados

Detalhamento:

Os ativos obtêm seu valor e importância por meio de sua associação com os aspectos das operações da <Instituição> que suportam. Ativos de TO são componentes de hardware e software que compõem os Sistemas de Controle Industrial (ICS). Diferentemente dos ativos de TI, esses dispositivos são projetados para durabilidade em condições extremas e operação em tempo real. Identificar e inventariar ativos de TO de alto valor ajuda a possibilitar a seleção e aplicação de controles apropriados. a <Instituição> deve considerar os diferentes tipos de ativos de TO.

Os tipos de ativos de TO mais conhecidos, organizados por sua função no processo, são:

1. Controladores: dispositivos que executam a lógica de controle e tomam decisões automáticas no "chão de fábrica".

• PLC (Controlador Lógico Programável): ativo de TO mais comum, consiste em um computador robusto que recebe dados de sensores e envia comandos para atuadores.

• PAC (Controlador de Automação Programável): versão mais moderna e potente do PLC, capaz de lidar com tarefas complexas de computação e comunicação.

• DCS (Sistema de Controle Distribuído): usado em grandes plantas (refinarias, usinas), onde o controle não é centralizado em um único ponto, mas distribuído por diversos controladores interconectados.

2. Interface e Supervisão: ativos que permitem que os humanos interajam com as máquinas e visualizem o estado do processo.

• HMI (Interface Homem-Máquina): tela (ou painel) localizada próxima à máquina que permite ao operador monitorar dados e ajustar parâmetros manualmente.

• SCADA (Controle Supervisório e Aquisição de Dados): sistema de software de alto nível que coleta dados de vários PLCs e sensores, permitindo o controle de processos em grandes áreas geográficas (ex: redes de energia ou saneamento).

• Estação de Engenharia: computador usado para programar e configurar os PLCs e outros ativos de campo, sendo um dos pontos mais críticos para a segurança.

3. Dispositivos de Campo (Sensores e Atuadores): são os "olhos, ouvidos e mãos" do sistema de TO.

• Sensores: dispositivos que medem variáveis físicas (temperatura, pressão, vazão, vibração, nível).

• Atuadores: dispositivos que realizam a ação física (motores, válvulas, pistões pneumáticos, relés).

• RTU (Unidade Terminal Remota): dispositivo que coleta dados de sensores em locais remotos (como um poste de energia ou um duto) e os envia para o SCADA via rádio ou satélite.

4. Infraestrutura de Rede Industrial: diferentemente dos roteadores domésticos, esses ativos são feitos para suportar calor, poeira e interferência eletromagnética.

• Switches Industriais: dispositivos que gerenciam o tráfego de dados entre PLCs e IHMs, muitas vezes usando protocolos como Modbus TCP ou Profinet.

• Gateway Industrial: traduzem protocolos diferentes (ex: converte um sinal Serial antigo para Ethernet).

• Firewalls Industriais: ativos de segurança que entendem protocolos de TO e protegem a zona de controle contra acessos não autorizados.

Um bom inventário de hardware deve conter informações como:

1. Identificação e Rastreamento

Informações que permitem diferenciar um equipamento de outro inequivocamente.

• Hostname (Nome do Dispositivo): O nome de rede do equipamento.

• Número de Série (Serial Number): O identificador único de fábrica (crucial para garantias).

• Etiqueta de Patrimônio: O número de controle interno da sua empresa (aquela etiqueta colada fisicamente).

• Endereço MAC: A "impressão digital" da placa de rede. Essencial para rastreio em logs de DHCP ou Firewall.

• Endereço IP: O endereço lógico atual (se for estático, é ainda mais importante registrar).

2. Especificações Técnicas (Capacidade)

Informações necessárias para o planejamento de upgrades e suporte técnico.

• Fabricante e Modelo: (Ex: Dell Latitude 5420).

• Processador (CPU): Tipo e velocidade.

• Memória RAM: Quantidade total instalada.

• Armazenamento (Disco): Tipo (SSD/HDD) e capacidade total.

• Sistema Operacional e Versão: (Ex: Windows 10 Pro 22H2).

• BIOS/Firmware: Versão atual (crítico para corrigir vulnerabilidades de segurança de baixo nível).

3. Interfaces e Interdependências

Informações necessárias para o planejamento de upgrades e substituições.

• Nome/identificador único da interface que identifique a conexão.

• Tipo de interface (natureza da conexão).

• Identificação dos ativos conectados: ativo(s) fonte/cliente; ativo(s) destino/servidor.

• Propósito da interface

• Criticidade/nível de dependência

• Protocolo(s) e porta(s) utilizado(s)

• Direção do tráfego: inbound, outbound ou bidirecional

4. Localização e Propriedade (Responsabilidade)

Informações fundamentais para auditorias físicas e recuperação de equipamentos.

• Responsável: Quem utiliza o equipamento primariamente.

• Departamento/Centro de Custo: Quem paga pelo equipamento.

• Localização Física: Escritório, Andar, Sala ou, no caso de trabalho remoto, a cidade/estado do colaborador.

• Status do Ativo: Em uso, Em estoque (Disponível), Em manutenção, Aposentado/Descarte.

5. Ciclo de Vida e Financeiro (Gestão)

Informações que ajudam a evitar renovações desnecessárias ou perda de prazos de garantia ou suporte.

• Data de Compra: Para cálculo de depreciação.

• Data de Expiração da Garantia: Para saber se o conserto é custo zero ou pago.

• Fornecedor (Vendor): De quem foi comprado (para acionar suporte).

• Valor de Aquisição: Custo original.

• Data de Fim de Vida (EOL - End of Life): Quando o fabricante parará de dar suporte ou atualizações.

E02-CIBERFÍSICOS-01-B

O inventário de ativos de TO inclui ativos dentro da <Instituição> que podem ser alavancados para alcançar um objetivo de ameaça

Detalhamento:

Ativos dentro da <Instituição> são aqueles que a <Instituição> considera como o alvo potencial das táticas ou objetivos de um agente de ameaças. Ao considerar ativos que deveriam receber essa designação, é útil considerar ativos que um agente de ameaças poderia usar para alcançar seu objetivo final, como:

• Ativos voltados para o público que podem servir como ponto de acesso inicial

• Ativos individuais que permitiriam movimento lateral dentro da rede da <Instituição>

• Ativos com direitos administrativos que possibilitariam a escalada de privilégios

Note que a identificação desse conjunto de ativos deve ser baseada em uma avaliação de risco e pode ser informada pelo entendimento da exposição da <Instituição> a ameaças e vulnerabilidades, na medida em que estas sejam conhecidas.

E02-CIBERFÍSICOS-01-C

Ativos de TO inventariados são priorizados com base em critérios definidos que incluem importância para a entrega da <Instituição>

Detalhamento:

A priorização dos ativos é importante para muitas atividades operacionais e de cibersegurança, como resposta a incidentes, gestão de riscos, gestão de ameaças e planejamento da arquitetura de cibersegurança. Existem múltiplas abordagens para priorização de ativos: classificação forçada (lista sequencial), classificação em níveis (por exemplo, todos os ativos lidando com o fluxo de gás são de nível 1, ativos relacionados à eficiência e monitoramento são de nível 2, e funções não críticas como relações públicas e marketing são de nível 3). Os níveis devem ser baseados em critérios definidos, como importância do ativo para a <Instituição> (por exemplo, segurança, criticidade do ativo para a entrega da <Instituição>, escassez do ativo, quão dependentes outros ativos são desse ativo) ou a sensibilidade dos dados armazenados ou processados pelo ativo. As prioridades devem ser documentadas e, idealmente, acordadas por todas as partes interessadas envolvidas. Eles também devem ser comunicados em toda a <Instituição> para uso em resposta a incidentes, gestão de riscos e outras atividades relevantes. Por exemplo, ativos virtualizados podem apresentar risco aumentado devido a questões como expansão dos ativos e suas características únicas (facilidade de captura de instantâneos e armazenamento de máquinas virtuais dormentes como arquivos) e, portanto, podem representar maior risco para a <Instituição>. Qualquer que seja a abordagem utilizada, a importância do ativo para a entrega da <Instituição> deve ser um dos critérios de priorização utilizados.

E02-CIBERFÍSICOS-01-D

Os critérios de priorização incluem a consideração do grau em que um ativo dentro da <Instituição> pode ser aproveitado para alcançar um objetivo de ameaça

Detalhamento:

A possibilidade de um ativo ser alavancado para alcançar um objetivo de ameaça é adicionada aos critérios para priorizar ativos de TO. É importante considerar que um agente de ameaças pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes situações. Incluir critérios adicionais além daqueles usados para ativos importantes para a execução da <Instituição> permitirá uma priorização mais abrangente dos riscos e impactos associados aos ativos de TO.

E02-CIBERFÍSICOS-01-E

O inventário de TO inclui atributos que suportam atividades de cibersegurança (por exemplo, localização, prioridade de ativos, proprietário do ativo, sistema operacional e versões de firmware)

Detalhamento:

Atributos de inventário são detalhes sobre ativos incluídos nos inventários de ativos para permitir a gestão e o uso consistente dos ativos. Incluir informações necessárias sobre ativos para apoiar as atividades do programa de cibersegurança ajuda a garantir que essas informações estejam disponíveis durante períodos de estresse operacional e não precisem ser coletadas em estado de crise. Por exemplo, os respondentes de incidentes poderão identificar facilmente a prioridade, criticidade e localização das máquinas que são afetadas por um evento de bloqueio e precisam ser substituídas.

Além disso, atributos de inventário podem ser usados para indicar aspectos de ativos que podem exigir atenção ou tratamento especial, como sistemas que utilizam inteligência artificial ou aprendizado de máquina. Exemplos de atributos potenciais de inventário incluem localizações físicas, localizações de rede, importância para a entrega da <Instituição>, impacto em caso de violação, datas de fim de vida, datas de fim de suporte, sistema operacional, firmware, versões.

E02-CIBERFÍSICOS-01-F

O inventário de ativos de TO está completo (o inventário inclui todos os ativos da <Instituição>)

Detalhamento:

Esta <Ação> amplia o escopo do inventário. Qualquer ativo de TO relacionado à entrega da <Instituição> deve ser identificado e inventariado, junto com seus atributos. A relação entre ativos e funções empresariais também deve ser incluída para permitir a priorização e o desenvolvimento de estratégias de proteção e sustentação. A implementação do inventário deve ser proporcional ao tamanho, complexidade e risco da <Instituição>. Por exemplo, para uma empresa pequena e de baixa complexidade, uma planilha simples pode ser usada para o estoque. Para empresas maiores e mais complexas, métodos mais sofisticados, como a aplicação dedicada de inventário de ativos, são apropriados. a <Instituição> pode considerar implementar ferramentas para identificar quais dispositivos estão conectados às redes e identificar novas conexões inesperadas.

a <Instituição> deve considerar os diferentes tipos de ativos de TO que podem estar dentro do escopo da autoavaliação, tais como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem (público, híbrido ou privado de serviço, software como serviço, plataforma como serviço e infraestrutura como serviço etc.)

• Ativos móveis

• Ativos de campo

• Ativos de backup, sobressalentes e redundantes, incluindo ativos virtualizados inativos

• Ativos dependentes de infraestrutura específica como redes sem fio, serviços de navegação e temporização de posicionamento, e os ativos do Sistema de Posição Global que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas

Inventário refere-se a uma listagem completa e não pretende implicar que uma única lista seja necessária; Múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, entretanto, a <Instituição> deve considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios. As

tecnologias de descoberta de ativos estão aumentando em capacidade e disponibilidade e podem ser aproveitadas para realizar esta <Ação>.

E02-CIBERFÍSICOS-01-G

O inventário de ativos de TO está atualizado, ou seja, é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema

Detalhamento:

O inventário de ativos e componentes significativos deve ser atualizado e mantido conforme os ativos mudam ao longo de seu ciclo de vida para garantir que o inventário seja completo e preciso. Garantir que o estoque de ativos esteja atualizado pode envolver procedimentos de gerenciamento de mudanças que exigem atualizações de estoque sempre que os ativos são trocados ou significativamente alterados. a <Instituição> também pode realizar revisões de estoque, tanto periodicamente (como trimestral ou anualmente) quanto com base em eventos (como mudanças na estrutura organizacional, grandes mudanças na infraestrutura tecnológica e aquisição e consolidação de outro negócio). a <Instituição> pode considerar implementar ferramentas que possibilitem a descoberta automatizada de ativos e forneçam uma compreensão mais em tempo real dos inventários.

E02-CIBERFÍSICOS-02

Gerenciar a configuração de ativos de hardware de TO

E02-CIBERFÍSICOS-02-A

As linhas de base de configuração são estabelecidas

Detalhamento:

Estabelecer uma linha de base para ativos TO, TI e informacionais fornece uma base para gerenciar a integridade dos ativos à medida que mudam ao longo de seu ciclo de vida. Estabelecer capturas pontuais-in-tempo dos ativos (itens de configuração) garante que esses ativos possam ser restaurados a uma forma aceitável quando necessário — após uma interrupção, quando ocorreu uma modificação não autorizada ou em qualquer circunstância em que a integridade seja duvidosa e forneça um nível de controle sobre mudanças que possam potencialmente prejudicar o suporte dos ativos aos serviços organizacionais.

a <Instituição> pode considerar mecanismos de verificação de integridade (manual ou automática) ao realizar capturas pontuais-in-tempo de ativos e configurações de ativos. O uso de mecanismos de verificação de integridade para verificar capturas em um momento específico antes da restauração pode ajudar a garantir que elas sejam viáveis e disponíveis.

Políticas e procedimentos documentados para a configuração ou manutenção de linhas de base não são obrigatórios para implementar esta <Ação>.

E02-CIBERFÍSICOS-02-B

Linhas de base de configuração são usadas para configurar ativos na implantação e restauração

Detalhamento:

A <Instituição> possui procedimentos para garantir que linhas de base de configuração estabelecidas sejam aplicadas aos ativos quando eles são implantados e restaurados. Essas linhas de base (também chamadas de builds padrão) suportam o deslocamento de ativos de forma controlada.

E02-CIBERFÍSICOS-02-C

As linhas de base de configuração incorporam os requisitos aplicáveis da arquitetura de cibersegurança

Detalhamento:

Como parte da arquitetura de cibersegurança, a <Instituição> seleciona e documenta os requisitos para o nível adequado de confidencialidade, integridade e disponibilidade de ativos de TI, TO e informação. Esses requisitos podem então ser usados para impulsionar o desenvolvimento de controles de cibersegurança a serem aplicados a ativos e sistemas (como linhas de base de configuração, proteções de rede, segurança de software). Diretrizes de reforço da linha de base de configuração, como os Center for Internet Security Benchmarks ou os Guias Técnicos de Implementação de Segurança (STIGs) do Departamento de Defesa, podem fornecer um ponto de partida para selecionar configurações que atendam aos requisitos da arquitetura de cibersegurança.

E02-CIBERFÍSICOS-02-D

As linhas de base de configuração são revisadas e atualizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e alterações na arquitetura de cibersegurança

Detalhamento:

A <Instituição> possui um cronograma definido para revisar regularmente as linhas de base e atualizá-las conforme necessário, garantindo que continuem refletindo requisitos adequados de segurança e funcionalidade.

E02-CIBERFÍSICOS-02-E

As configurações dos ativos são monitoradas para garantir consistência com as linhas de base ao longo dos ciclos de vida dos ativos

Detalhamento:

a <Instituição> deve monitorar as configurações dos ativos para garantir que continuem a se conformar às linhas de base ao longo do tempo após a implantação. O monitoramento de consistência pode ser feito por meios automatizados, como o uso de uma ferramenta de varredura que compare as linhas de base dos ativos conectados com as linhas de configuração estabelecidas, ou realizando auditorias periódicas dos ativos para determinar se mudanças não autorizadas foram feitas. Ferramentas também podem ser usadas para reverter automaticamente os ativos para referências.

Ferramentas automatizadas de gerenciamento de configuração ou monitoramento podem permitir um rastreamento mais eficiente das configurações dos ativos. Ferramentas capazes de abranger ambientes físicos, virtuais, móveis, híbridos e outros ambientes tecnológicos devem ser consideradas para ajudar a garantir cobertura adequada dos ativos de TI. Essas ferramentas podem ser otimizadas para produtos específicos. Ao selecionar ferramentas de automação, os stakeholders com treinamento e experiência adequados devem ser engajados desde cedo e deve ser dada uma consideração cuidadosa para garantir a adequação adequada entre as ferramentas de automação e os produtos com os quais elas se destinam a integrar.

Ferramentas de integridade de dados (como checksums criptográficos) podem ajudar na detecção de alterações não autorizadas nas configurações de configuração, especialmente ao gerenciar ativos virtualizados. Como exemplo disso, uma <Instituição> pode implementar verificações de integridade de arquivos para plataformas de virtualização a serem realizadas na inicialização e confirmar que nenhuma alteração não autorizada ocorreu.

E02-CIBERFÍSICOS-03

Gerenciar alterações nos ativos de hardware de TO

E02-CIBERFÍSICOS-03-A

Mudanças nos ativos são avaliadas e aprovadas antes de serem implementadas

Detalhamento:

Todas as mudanças propostas nos ativos inventariados são avaliadas para entender sua prioridade, benefícios, riscos e impactos na funcionalidade e segurança das funções que suportam. Considere que eles podem variar entre diferentes tipos de ativos, como:

- Ativos virtualizados
- Ativos regulados
- Ativos gerenciados por terceiros
- Ativos BYOD
- Ativos em nuvem
- Ativos móveis
- Ativos de campo
- Ativos dependentes de infraestrutura específica como redes sem fio ou o Sistema Global de Posição
- Ativos que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas.

E02-CIBERFÍSICOS-03-B

Mudanças nos ativos são documentadas

Detalhamento:

Quaisquer alterações feitas em um ativo inventariado são capturadas em um formato que pode ser facilmente referenciado durante atividades de resolução de problemas ou resposta a incidentes. As mudanças podem incluir a alteração de configurações como roteamento e configurações de portas em dispositivos de rede, a adição ou remoção de componentes e a modificação de privilégios de acesso. Alguns dos atributos que devem ser registrados incluem data e hora da mudança, quem fez a alteração, os ativos afetados pela mudança e uma descrição de quaisquer riscos associados à mudança.

E02-CIBERFÍSICOS-03-C

Os requisitos de documentação para alterações de ativos são estabelecidos e mantidos

Detalhamento:

A <Instituição> deve definir as informações necessárias que devem ser documentadas ao realizar mudanças nos ativos de TO. Os requisitos devem considerar quais informações podem ser necessárias para atividades como solução de problemas ou resposta a incidentes.

Além disso, a <Instituição> deve considerar a manutenção desses requisitos com base nas mudanças no ambiente operacional.

E02-CIBERFÍSICOS-03-D

Mudanças em ativos de prioridade mais alta são testadas antes de serem implantadas

Detalhamento:

Mudanças nos ativos devem ser testadas para garantir a continuidade dos ativos e funções que afetam antes de implementar as mudanças em toda a empresa. Quando possível, os testes das mudanças propostas devem ser realizados em um ambiente de teste ou em um ambiente de produção de baixo risco. Os testes podem incluir testes de estresse, confirmação de que mudanças foram implementadas, operabilidade e testes de carga.

Além disso, a <Instituição> pode considerar se controles que impedem mudanças não autorizadas são necessários para tipos específicos de ativos. Por exemplo, interruptores de programação digitais ou de hardware devem ser colocados em um modo que não permita programação durante operações rotineiras.

E02-CIBERFÍSICOS-03-E

Mudanças e atualizações são implementadas de forma segura

Detalhamento:

Procedimentos e ferramentas usados para atualizar ativos devem incorporar controles apropriados para garantir que vulnerabilidades ou configurações incorretas ou não intencionais sejam introduzidas como parte dos processos de mudança de ativos. Isso pode incluir o uso de protocolos de comunicação segura, métodos de verificação, como assinaturas digitais, ou outros controles.

E02-CIBERFÍSICOS-03-F

A capacidade de reverter mudanças é estabelecida e mantida para ativos importantes para a execução da <Instituição>

Detalhamento:

Existe a capacidade de se reverter mudanças após sua aplicação. Isso pode ser alcançado por métodos manuais ou automatizados. Isso permite que uma <Instituição> volte a um estado conhecido de bom caso uma mudança crie consequências operacionais ou de segurança imprevistas ou não intencionais que não possam ser resolvidas por outros meios.

E02-CIBERFÍSICOS-03-G

As <Ações> de gestão de mudanças abrangem todo o ciclo de vida dos ativos (por exemplo, aquisição, implantação, operação, aposentadoria)

Detalhamento:

As condições organizacionais e operacionais estão em constante mudança, resultando em mudanças na equipe, no conteúdo e uso dos dados, na tecnologia, entre outros. Essas mudanças podem impactar ativos importantes ao longo de seus ciclos de vida. As <Ações> de gestão de mudanças não devem se limitar a mudanças nos ativos operacionalmente implantados, mas devem abranger todas as fases do ciclo de vida, incluindo aquisição, implantação e aposentadoria.

Para isso, a <Instituição> deve definir e gerenciar o processo para manter o inventário de ativos atualizado e garantir que mudanças no estoque não resultem em lacunas nas estratégias para proteger e manter os ativos.

Além disso, a <Instituição> deve monitorar ativamente mudanças que alterem significativamente os ativos, identificar novos ativos e pedir a aposentadoria de ativos para os quais não há mais necessidade ou cujo valor relativo foi reduzido.

Considere que diferentes tipos de tecnologias (como ativos virtualizados e ativos em nuvem) podem ter estágios únicos do ciclo de vida e outros aspectos distintos que impactam como a gestão de mudanças deve ser implementada.

E02-CIBERFÍSICOS-03-H

Mudanças em ativos de prioridade mais alta são testadas quanto ao impacto em cibersegurança antes de serem implantadas

Detalhamento:

Alterações em um ativo usado em múltiplos serviços podem atender a uma necessidade imediata, mas causar problemas em outras aplicações. As mudanças devem ser avaliadas em um ambiente de teste para identificar qualquer impacto da mudança proposta em outros ativos e sistemas. O impacto na cibersegurança pode incluir qualquer impacto na disponibilidade de um ativo para usuários autorizados, enfraquecimento das proteções ou alterações não intencionais nas listas de controle de acesso. Por exemplo, se um fornecedor lança uma nova versão de um sistema operacional, o novo sistema operacional deve ser testado em um ambiente controlado para determinar se algum aplicativo ou serviço seria afetado.

E02-CIBERFÍSICOS-03-I

Os registros de alterações incluem informações sobre modificações que impactam os requisitos de cibersegurança dos ativos

Detalhamento:

Se testes de impacto em cibersegurança antes da implantação de alterações nos ativos revelarem que os requisitos de cibersegurança (confidencialidade, integridade e disponibilidade) serão afetados, esses impactos devem ser descritos nos registros de alterações quando os ativos forem alterados. Por exemplo, se os esquemas de endereçamento IP forem alterados dentro de um dispositivo de rede, o registro de alterações deve indicar como a disponibilidade de dispositivos conectados pode ser afetada.

E02-CIBERFÍSICOS-04

Gerenciar inventário de ativos de software de TO

E02-CIBERFÍSICOS-04-A

Os ativos de software de TO importantes para a entrega da <Instituição> são inventariados

Detalhamento:

Os ativos obtêm seu valor e importância por meio de sua associação com os aspectos das operações da <Instituição> que suportam. Identificar e inventariar ativos de software de TO de alto valor ajuda a possibilitar a seleção e aplicação de controles apropriados. a <Instituição> deve considerar os diferentes tipos de ativos de software de TO que podem estar dentro do escopo da autoavaliação, coletando dados relevantes sobre o software, pois um inventário de software eficiente vai muito além de uma simples lista de nomes. Ele precisa fornecer contexto para segurança, licenciamento e suporte.

Aqui estão os elementos comuns e essenciais divididos por categorias:

1. Identificação Básica do Software: estes dados respondem "o que é isso?" e "quem o fez?".

• Nome do Software: Nome completo e comercial (ex: TIA Portal, Windows Server 2022).

• Versão e Build: Crucial para identificar se o software está atualizado ou vulnerável.

• Fabricante (Vendor): Quem fornece o suporte e as atualizações (ex: Siemens, Microsoft, Oracle).

• ID do Ativo (Tag): Um identificador único que vincula o software a um registro no banco de dados de ativos.

2. Contexto de Instalação e Localização: estes dados respondem "onde ele está rodando?".

• Hostname/Dispositivo: Nome do servidor, workstation ou PLC onde o software reside.

• Caminho de Instalação (Path): Localização no diretório do sistema (importante para detectar executáveis maliciosos).

• Ambiente: Se o software está em Produção, Homologação ou Desenvolvimento.

• Tipo de Instalação: Se é local, SaaS (nuvem), máquina virtual ou container.

3. Gestão de Segurança e Vulnerabilidades: estes dados são essenciais para os <Eixos> AMEAÇAS e CONFIGURAÇÃO.

• Status de Suporte (EOL/EOS): Indica se o software já chegou ao fim da vida útil (End of Life) ou fim do suporte, o que representa um risco crítico.

• CVEs Conhecidas: Lista de vulnerabilidades associadas àquela versão específica.

• Nível de Criticidade: Qual o impacto para o negócio se esse software parar ou for invadido?

• Assinatura Digital: Se o executável é assinado e verificado por um fornecedor confiável.

4. Gestão de Licenciamento e Conformidade: estes dados são focados em custos e aspectos legais.

• Tipo de Licença: (SaaS, Perpétua, Open Source, Freeware).

• Data de Expiração: quando a licença ou o contrato de manutenção precisa ser renovado.

• Quantidade de Instalações: quantas instâncias estão em uso vs. quantas foram adquiridas.

• Requisitos de Atualização (Patch): se o software aceita atualizações automáticas ou exige intervenção manual (janela de manutenção).

==========

Elementos Específicos para Software de TO (Tecnologia Operacional)

Ativos de TO demandam informações particularidades:

• Versão do Firmware: para controladores (PLCs) o firmware é o "software" principal.

• Protocolos de Comunicação: quais protocolos o software utiliza (Modbus, Profinet, etc).

• Dependência de Hardware: se o software demanda uma versão específica de hardware proprietário.

• Dependência de Software: se o software demanda uma versão específica de software (proprietário ou comercial).

==========

É importante atentar para ativos que têm potencial para não serem rastreados, não reclamados ou de outra forma negligenciados, como ativos legados, equipamentos de comunicação e ativos que suportam múltiplos grupos

Um inventário não implica que uma única lista seja necessária; múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, a <Instituição> deve,

entretanto, considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios.

E02-CIBERFÍSICOS-04-B

O inventário de ativos de software de TO inclui ativos dentro da <Instituição> que podem ser alavancados para alcançar um objetivo de ameaça

Detalhamento:

Ativos dentro da <Instituição> são aqueles que a <Instituição> considera como o alvo potencial das táticas ou objetivos de um agente de ameaças. Ao considerar ativos que deveriam receber essa designação, é útil considerar ativos que um agente de ameaças poderia usar para alcançar seu objetivo final, como:

• Ativos voltados para o público que podem servir como ponto de acesso inicial

• Ativos individuais que permitiriam movimento lateral dentro da rede da <Instituição>

• Ativos com direitos administrativos que possibilitariam a escalada de privilégios

Note que a identificação desse conjunto de ativos deve ser baseada em uma avaliação de risco e pode ser informada pelo entendimento da exposição da <Instituição> a ameaças e vulnerabilidades, na medida em que estas sejam conhecidas.

E02-CIBERFÍSICOS-04-C

Ativos de software de TO inventariados são priorizados com base em critérios definidos que incluem importância para a entrega da <Instituição>

Detalhamento:

A priorização dos ativos é importante para muitas atividades operacionais e de cibersegurança, como resposta a incidentes, gestão de riscos, gestão de ameaças e planejamento da arquitetura de cibersegurança. Existem múltiplas abordagens para priorização de ativos: classificação forçada (lista sequencial), classificação em níveis (por exemplo, todos os ativos lidando com o fluxo de gás são de nível 1, ativos relacionados à eficiência e monitoramento são de nível 2, e funções não críticas como relações públicas e marketing são de nível 3).

Os níveis devem ser baseados em critérios definidos, como importância do ativo para a <Instituição> (por exemplo, segurança, criticidade do ativo para a entrega da <Instituição>, escassez do ativo, quão dependentes outros ativos são desse ativo) ou a sensibilidade dos dados armazenados ou processados pelo ativo.

As prioridades devem ser documentadas e, idealmente, acordadas por todas as partes interessadas envolvidas. Eles também devem ser comunicados em toda a <Instituição> para uso em resposta a incidentes, gestão de riscos e outras atividades relevantes.

Por exemplo, ativos virtualizados podem apresentar risco aumentado devido a questões como expansão dos ativos e suas características únicas (facilidade de captura de instantâneos e armazenamento de máquinas virtuais dormentes como arquivos) e, portanto, podem representar maior risco para a <Instituição>.

Qualquer que seja a abordagem utilizada, a importância do ativo para a entrega da <Instituição> deve ser um dos critérios de priorização utilizados.

E02-CIBERFÍSICOS-04-D

Os critérios de priorização incluem a consideração do grau em que um ativo dentro da <Instituição> pode ser aproveitado para alcançar um objetivo de ameaça

Detalhamento:

A possibilidade de um ativo ser alavancado para alcançar um objetivo de ameaça é adicionada aos critérios para priorizar ativos de software de TI. É importante considerar que um agente de ameaças pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes situações. Incluir critérios adicionais além daqueles usados para ativos importantes para a execução da <Instituição> permitirá uma priorização mais abrangente dos riscos e impactos associados aos ativos de software de TI.

E02-CIBERFÍSICOS-04-E

O inventário de TO inclui atributos que suportam atividades de cibersegurança (por exemplo, localização, prioridade de ativos, proprietário do ativo, sistema operacional e versões de firmware)

Detalhamento:

Atributos de inventário são detalhes sobre ativos incluídos nos inventários de ativos para permitir a gestão e o uso consistente dos ativos. Incluir informações necessárias sobre ativos para apoiar as atividades do programa de cibersegurança ajuda a garantir que essas informações estejam disponíveis durante períodos de estresse operacional e não precisem ser coletadas em estado de crise. Por exemplo, os respondentes de incidentes poderão identificar facilmente a prioridade, criticidade e localização das máquinas que são afetadas por um evento de bloqueio e precisam ser substituídas.

Além disso, atributos de inventário podem ser usados para indicar aspectos de ativos que podem exigir atenção ou tratamento especial, como sistemas que utilizam inteligência artificial ou aprendizado de máquina. Exemplos de atributos potenciais de inventário incluem localizações físicas, localizações de rede, importância para a entrega da <Instituição>, impacto em caso de violação, datas de fim de vida, datas de fim de suporte, sistema operacional, firmware, versões.

E02-CIBERFÍSICOS-04-F

O inventário de ativos de software de TI está completo (o inventário inclui todos os ativos da <Instituição>)

Detalhamento:

Esta <Ação> amplia o escopo do inventário. Qualquer ativo de TO relacionado à entrega da <Instituição> deve ser identificado e inventariado, junto com seus atributos. A relação entre ativos e funções empresariais também deve ser incluída para permitir a priorização e o desenvolvimento de estratégias de proteção e sustentação.

A implementação do inventário deve ser proporcional ao tamanho, complexidade e risco da <Instituição>. Por exemplo, para uma empresa pequena e de baixa complexidade, uma planilha simples pode ser usada para o estoque. Para empresas maiores e mais complexas, métodos mais sofisticados, como a aplicação dedicada de inventário de ativos, são apropriados. a <Instituição> pode considerar implementar ferramentas para identificar quais dispositivos estão conectados às redes e identificar novas conexões inesperadas.

A <Instituição> deve considerar os diferentes tipos de ativos de software de TO que podem estar dentro do escopo da autoavaliação, tais como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem (público, híbrido ou privado de serviço, software como serviço, plataforma como serviço e infraestrutura como serviço etc.)

• Ativos móveis

• Ativos de campo

• Ativos de backup, sobressalentes e redundantes, incluindo ativos virtualizados inativos

• Ativos dependentes de infraestrutura específica como redes sem fio, serviços de navegação e temporização de posicionamento, e os ativos do Sistema de Posição Global que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas

Inventário refere-se a uma listagem completa e não pretende implicar que uma única lista seja necessária; múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, entretanto, a <Instituição> deve considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios. As tecnologias de descoberta de ativos estão aumentando em capacidade e disponibilidade e podem ser aproveitadas para realizar esta <Ação>.

E02-CIBERFÍSICOS-04-G

O inventário de ativos de software de TO está atualizado, ou seja, é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema

Detalhamento:

O inventário de ativos e componentes significativos deve ser atualizado e mantido conforme os ativos mudam ao longo de seu ciclo de vida para garantir que o inventário seja completo e preciso. Garantir que o estoque de ativos esteja atualizado pode envolver procedimentos de gerenciamento de mudanças que exigem atualizações de estoque sempre que os ativos são trocados ou significativamente alterados. a <Instituição> também pode realizar revisões de estoque, tanto periodicamente (como trimestral ou anualmente) quanto com base em eventos (como mudanças na estrutura organizacional, grandes mudanças na infraestrutura tecnológica e aquisição e consolidação de outro negócio). a <Instituição> pode considerar implementar ferramentas que possibilitem a descoberta automatizada de ativos e forneçam uma compreensão mais em tempo real dos inventários.

E02-CIBERFÍSICOS-05

Gerenciar a configuração de ativos de software de TO

E02-CIBERFÍSICOS-05-A

As linhas de base de configuração são estabelecidas

Detalhamento:

Estabelecer uma linha de base para ativos TO fornece uma base para gerenciar a integridade dos ativos à medida que mudam ao longo de seu ciclo de vida. Estabelecer capturas pontuais-in-tempo dos ativos (itens de configuração) garante que esses ativos possam ser restaurados a uma forma aceitável quando necessário — após uma interrupção, quando ocorreu uma modificação não autorizada ou em qualquer

circunstância em que a integridade seja duvidosa e forneça um nível de controle sobre mudanças que possam potencialmente prejudicar o suporte dos ativos aos serviços organizacionais.

a <Instituição> pode considerar mecanismos de verificação de integridade (manual ou automática) ao realizar capturas pontuais-in-tempo de ativos e configurações de ativos. O uso de mecanismos de verificação de integridade para verificar capturas em um momento específico antes da restauração pode ajudar a garantir que elas sejam viáveis e disponíveis.

Políticas e procedimentos documentados para a configuração ou manutenção de linhas de base não são obrigatórios para implementar esta <Ação>.

E02-CIBERFÍSICOS-05-B

Linhas de base de configuração são usadas para configurar ativos na implantação e restauração

Detalhamento:

A <Instituição> possui procedimentos para garantir que linhas de base de configuração estabelecidas sejam aplicadas aos ativos quando eles são implantados e restaurados. Essas linhas de base (também chamadas de builds padrão) suportam o deslocamento de ativos de forma controlada.

E02-CIBERFÍSICOS-05-C

As linhas de base de configuração incorporam os requisitos aplicáveis da arquitetura de cibersegurança

Detalhamento:

Como parte da arquitetura de cibersegurança, a <Instituição> seleciona e documenta os requisitos para o nível adequado de confidencialidade, integridade e disponibilidade de ativos de software de TO. Esses requisitos podem então ser usados para impulsionar o desenvolvimento de controles de cibersegurança a serem aplicados a ativos e sistemas (como linhas de base de configuração, proteções de rede, segurança de software). Diretrizes de reforço da linha de base de configuração, como os Center for Internet Security Benchmarks ou os Guias Técnicos de Implementação de Segurança (STIGs) do Departamento de Defesa, podem fornecer um ponto de partida para selecionar configurações que atendam aos requisitos da arquitetura de cibersegurança.

E02-CIBERFÍSICOS-05-D

As linhas de base de configuração são revisadas e atualizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e alterações na arquitetura de cibersegurança

Detalhamento:

A <Instituição> possui um cronograma definido para revisar regularmente as linhas de base e atualizá-las conforme necessário, garantindo que continuem refletindo requisitos adequados de segurança e funcionalidade.

E02-CIBERFÍSICOS-05-E

As configurações dos ativos são monitoradas para garantir consistência com as linhas de base ao longo dos ciclos de vida dos ativos

Detalhamento:

A <Instituição> deve monitorar as configurações dos ativos para garantir que continuem a se conformar às linhas de base ao lo+F78ngo do tempo após a implantação. O monitoramento de consistência pode ser feito por meios automatizados, como o uso de uma ferramenta de varredura que compare as linhas de base dos ativos conectados com as linhas de configuração estabelecidas, ou realizando auditorias periódicas dos ativos para determinar se mudanças não autorizadas foram feitas. Ferramentas também podem ser usadas para reverter automaticamente os ativos para referências.

Ferramentas automatizadas de gerenciamento de configuração ou monitoramento podem permitir um rastreamento mais eficiente das configurações dos ativos. Ferramentas capazes de abranger ambientes físicos, virtuais, móveis, híbridos e outros ambientes tecnológicos devem ser consideradas para ajudar a garantir cobertura adequada dos ativos de software de TI. Essas ferramentas podem ser otimizadas para produtos específicos. Ao selecionar ferramentas de automação, os stakeholders com treinamento e experiência adequados devem ser engajados desde cedo e deve ser dada uma consideração cuidadosa para garantir a adequação adequada entre as ferramentas de automação e os produtos com os quais elas se destinam a integrar.

Ferramentas de integridade de dados (como checksums criptográficos) podem ajudar na detecção de alterações não autorizadas nas configurações de configuração, especialmente ao gerenciar ativos virtualizados. Como exemplo disso, uma <Instituição> pode implementar verificações de integridade de arquivos para plataformas de virtualização a serem realizadas na inicialização e confirmar que nenhuma alteração não autorizada ocorreu.

E02-CIBERFÍSICOS-06

Gerenciar alterações nos ativos de software de TO

E02-CIBERFÍSICOS-06-A

Mudanças nos ativos são avaliadas e aprovadas antes de serem implementadas

Detalhamento:

Todas as mudanças propostas nos ativos inventariados são avaliadas para entender sua prioridade, benefícios, riscos e impactos na funcionalidade e segurança das funções que suportam. Considere que eles podem variar entre diferentes tipos de ativos de TO, TO e de informação, como:

• Ativos virtualizados

• Ativos regulados

• Ativos gerenciados por terceiros

• Ativos BYOD

• Ativos em nuvem

• Ativos móveis

• Ativos de campo

• Ativos dependentes de infraestrutura específica como redes sem fio ou o Sistema Global de Posição

• Ativos que podem ser considerados parte da Internet das Coisas ou Internet Industrial das Coisas.

E02-CIBERFÍSICOS-06-B

Mudanças nos ativos são documentadas

Detalhamento:

Quaisquer alterações feitas em um ativo inventariado são capturadas em um formato que pode ser facilmente referenciado durante atividades de resolução de problemas ou resposta a incidentes. As mudanças podem incluir a alteração de configurações como roteamento e configurações de portas em dispositivos de rede, a adição ou remoção de componentes e a modificação de privilégios de acesso. Alguns dos atributos que devem ser registrados incluem data e hora da mudança, quem fez a alteração, os ativos afetados pela mudança e uma descrição de quaisquer riscos associados à mudança.

E02-CIBERFÍSICOS-06-C

Os requisitos de documentação para alterações de ativos são estabelecidos e mantidos

Detalhamento:

A <Instituição> deve definir as informações necessárias que devem ser documentadas ao realizar mudanças nos ativos de TO. Os requisitos devem considerar quais informações podem ser necessárias para atividades como solução de problemas ou resposta a incidentes.

Além disso, a <Instituição> deve considerar a manutenção desses requisitos com base nas mudanças no ambiente operacional.

E02-CIBERFÍSICOS-06-D

Mudanças em ativos de prioridade mais alta são testadas antes de serem implantadas

Detalhamento:

Mudanças nos ativos devem ser testadas para garantir a continuidade dos ativos e funções que afetam antes de implementar as mudanças em toda a empresa. Quando possível, os testes das mudanças propostas devem ser realizados em um ambiente de teste ou em um ambiente de produção de baixo risco. Os testes podem incluir testes de estresse, confirmação de que mudanças foram implementadas, operabilidade e testes de carga.

Além disso, a <Instituição> pode considerar se controles que impedem mudanças não autorizadas são necessários para tipos específicos de ativos. Por exemplo, interruptores de programação digitais ou de hardware devem ser colocados em um modo que não permita programação durante operações rotineiras.

E02-CIBERFÍSICOS-06-E

Mudanças e atualizações são implementadas de forma segura

Detalhamento:

Procedimentos e ferramentas usados para atualizar ativos devem incorporar controles apropriados para garantir que vulnerabilidades ou configurações incorretas ou não intencionais sejam introduzidas como parte dos processos de mudança de ativos. Isso pode incluir o uso de protocolos de comunicação segura, métodos de verificação, como assinaturas digitais, ou outros controles.

E02-CIBERFÍSICOS-06-F

A capacidade de reverter mudanças é estabelecida e mantida para ativos importantes para a execução da <Instituição>

Detalhamento:

Esta <Ação> descreve o desenvolvimento da capacidade de reverter mudanças após sua aplicação. Isso pode ser alcançado por métodos manuais ou automatizados. Isso permite que uma <Instituição> volte a um estado conhecido de bom caso uma mudança crie consequências operacionais ou de segurança imprevistas ou não intencionais que não possam ser resolvidas por outros meios.

E02-CIBERFÍSICOS-06-G

As <Ações> de gestão de mudanças abrangem todo o ciclo de vida dos ativos (por exemplo, aquisição, implantação, operação, aposentadoria)

Detalhamento:

As condições organizacionais e operacionais estão em constante mudança, resultando em mudanças na equipe, no conteúdo e uso dos dados, na tecnologia, entre outros. Essas mudanças podem impactar ativos importantes ao longo de seus ciclos de vida. As <Ações> de gestão de mudanças não devem se limitar a mudanças nos ativos operacionalmente implantados, mas devem abranger todas as fases do ciclo de vida, incluindo aquisição, implantação e aposentadoria.

Para isso, a <Instituição> deve definir e gerenciar o processo para manter o inventário de ativos atualizado e garantir que mudanças no estoque não resultem em lacunas nas estratégias para proteger e manter os ativos.

Além disso, a <Instituição> deve monitorar ativamente mudanças que alterem significativamente os ativos, identificar novos ativos e pedir a aposentadoria de ativos para os quais não há mais necessidade ou cujo valor relativo foi reduzido.

Considere que diferentes tipos de tecnologias (como ativos virtualizados e ativos em nuvem) podem ter estágios únicos do ciclo de vida e outros aspectos distintos que impactam como a gestão de mudanças deve ser implementada.

E02-CIBERFÍSICOS-06-H

Mudanças em ativos de prioridade mais alta são testadas quanto ao impacto em cibersegurança antes de serem implantadas

Detalhamento:

Alterações em um ativo usado em múltiplos serviços podem atender a uma necessidade imediata, mas causar problemas em outras aplicações. As mudanças devem ser avaliadas em um ambiente de teste para identificar qualquer impacto da mudança proposta em outros ativos e sistemas. O impacto na cibersegurança pode incluir qualquer impacto na disponibilidade de um ativo para usuários autorizados, enfraquecimento das proteções ou alterações não intencionais nas listas de controle de acesso. Por exemplo, se um fornecedor lança uma nova versão de um sistema operacional, o novo sistema operacional deve ser testado em um ambiente controlado para determinar se algum aplicativo ou serviço seria afetado.

E02-CIBERFÍSICOS-06-I

Os registros de alterações incluem informações sobre modificações que impactam os requisitos de cibersegurança dos ativos

Detalhamento:

Se testes de impacto em cibersegurança antes da implantação de alterações nos ativos revelarem que os requisitos de cibersegurança (confidencialidade, integridade e disponibilidade) serão afetados, esses

impactos devem ser descritos nos registros de alterações quando os ativos forem alterados. Por exemplo, se os esquemas de endereçamento IP forem alterados dentro de um dispositivo de rede, o registro de alterações deve indicar como a disponibilidade de dispositivos conectados pode ser afetada.

E03-INFORMAÇÕES

Gerenciamento da Proteção de Ativos Informacionais

Resumo:

Estabelecer um programa de proteção informacional envolve identificar os requisitos de cibersegurança para os ativos informacionais da <Instituição> e projetar controles apropriados para protegê-los. A proteção informacional orienta como a cibersegurança deve ser implementada para atender aos objetivos da <Instituição>.

Detalhamento:

O <Eixo> Gerenciamento da Proteção de Ativos Informacionais é focado na <Instituição>. As <Ações> descritas em <Eixos> focados na <Instituição> são frequentemente executadas como parte de um programa de toda a <Instituição> e podem ser estabelecidas e operar independentemente da função no escopo. Para explicar isso, o objetivo inicial em cada <Eixo> focado na <Instituição> está focado no estabelecimento e manutenção do programa relacionado.

Informações (ativos informacionais) são todos os elementos de valor para uma <Instituição> que consistem em dados, informações ou conhecimentos coletados, gerados, armazenados, processados ou trafegados na <Instituição>. Eles abrangem desde bancos de dados, registros de clientes e segredos comerciais até manuais de processos e e-mails corporativos. Por serem cruciais para a continuidade do negócio e para a tomada de decisões, esses ativos exigem proteção rigorosa baseada nos princípios da confidencialidade, integridade, autenticidade e disponibilidade, garantindo que a informação esteja segura contra acessos não autorizados e permaneça precisa quando for necessária.

A estratégia de proteção de ativos informacionais é estabelecida como a base do gerenciamento. Em sua forma mais simples, a estratégia deve incluir um inventário de ativos informacionais e um plano para alcançá-los. Em níveis mais altos de maturidade, a estratégia será mais completa e incluirá prioridades, uma abordagem de governança, estrutura e implementação do processo e mais envolvimento da alta administração em seu desenho.

O gerenciamento da Proteção de Ativos Informacionais passa pela identificação, classificação, criptografia e prevenção de vazamento de ativos informacionais.

E03-INFORMAÇÕES-01

Gerenciar inventário de ativos de informações

E03-INFORMAÇÕES-01-A

Ativos de informação importantes para a entrega da <Instituição> (por exemplo, pontos de ajuste SCADA e informações do cliente) são inventariados

Detalhamento:

Os ativos obtêm seu valor e importância por meio de sua associação com os aspectos das operações da <Instituição> que suportam. Identificar e inventariar ativos de informação de alto valor ajuda a possibilitar a seleção e aplicação de controles apropriados. Ativos de alto valor também podem incluir ativos informativos que podem criar riscos financeiros, regulatórios ou de responsabilidade, como PII, informações operacionais sensíveis e informações empresariais confidenciais. a <Instituição> deve considerar os diferentes tipos de ativos que podem conter ativos informacionais informações importantes para a <Instituição>, tais como:

• Ativos virtualizados (incluindo ativos inativos e de backup)

• Ativos regulados

• Ativos em nuvem

• Ativos BYOD

• Ativos de campo

• Ativos móveis.

A <Instituição> também devem considerar diferentes fontes potenciais de informações de alto valor, tais como:

• Informações localizadas fora das instalações

• Informações armazenadas ou arquivadas

• Dados de backup

• Informações gerenciadas por terceiros

• Informações dentro de diferentes níveis de classificação ou sensibilidade

Um inventário não pretende implicar que uma única lista seja necessária; múltiplos repositórios, documentos ou sistemas podem ser usados para realizar esta <Ação>. Quando apropriado, entretanto, a <Instituição> deve considerar se os estoques podem ser consolidados para evitar riscos potenciais relacionados ao gerenciamento de múltiplos repositórios.

E03-INFORMAÇÕES-01-B

O inventário de ativos de informação inclui ativos de informação dentro da <Instituição> que podem ser aproveitados para alcançar um objetivo de ameaça

Detalhamento:

Esses são ativos que podem ser usados na busca das táticas ou objetivos de um ator de ameaça. É importante considerar que um ator ameaçador pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes situações. O cumprimento de um objetivo de ameaça pode não causar danos imediatos a uma <Instituição>, mas aumentaria a probabilidade de realização de um risco cibernético. A identificação de ativos dentro da <Instituição> que podem ser aproveitados para alcançar um objetivo de ameaça deve focar nas técnicas usadas pelos atores ameaçadores e no potencial dessas técnicas para serem aplicadas aos ativos da <Instituição>. Um exemplo de ativos dentro da <Instituição> que podem ser aproveitados para alcançar um objetivo de ameaça são informações como informações pessoalmente identificáveis que podem causar danos à <Instituição> ou aos seus stakeholders se forem perdidos, roubados ou divulgados.

Note que a identificação desse conjunto de ativos deve ser baseada em uma avaliação do risco.

E03-INFORMAÇÕES-01-C

Os ativos de informação inventariados são categorizados com base em critérios definidos que incluem importância para a entrega da <Instituição>

Detalhamento:

A categorização de ativos é importante para muitas atividades operacionais e de cibersegurança, como resposta a incidentes, gestão de riscos, gestão de ameaças e planejamento da arquitetura de cibersegurança.

As informações devem ser categorizadas de acordo com sua sensibilidade, valor, criticidade, interdependências com outros ativos, requisitos legais, se os dados são coletados, mantidos ou compartilhados com terceiros, ou outro esquema, incluindo qualquer esquema exigido por regulamentação ou outro fator de conformidade. A categorização fornece outro nível de descrição importante para um ativo de informação que pode afetar estratégias para protegê-lo e sustentá-lo.

Estes são exemplos de esquemas de categorização:

• Confidencial, Secreto, Ultrassecreto

• Regulado, Não Regulamentado, Público

• Restrito, Privado, Público

Qualquer que seja o esquema utilizado, a importância do ativo para a execução da <Instituição> deve ser considerada.

Além disso, ao identificar categorias, considere que muitas atividades de cibersegurança geram ativos de informação que precisam ser protegidos, como informações de linha de base de configuração, registros de risco e até mesmo inventários de ativos.

E03-INFORMAÇÕES-01-D

Os critérios de categorização incluem a consideração do grau em que um ativo dentro da <Instituição> pode ser aproveitado para alcançar um objetivo de ameaça

Detalhamento:

A possibilidade de um ativo dentro da <Instituição> ser aproveitado para alcançar um objetivo de ameaça é adicionada aos critérios usados para categorizar ativos de informação. Considerar como um ativo pode ser utilizado por um ator ameaçador permitirá uma priorização mais abrangente dos riscos e impactos associados aos ativos informacionais. É importante considerar que um ator ameaçador pode ter múltiplos objetivos e que esses objetivos podem mudar ao longo do tempo ou em diferentes situações.

E03-INFORMAÇÕES-01-E

O inventário de ativos de informação inclui atributos que apoiam atividades de cibersegurança (por exemplo, categoria de ativo, locais e frequências de backup, locais de armazenamento, proprietário do ativo, requisitos de cibersegurança)

Detalhamento:

Atributos de inventário de ativos de informação são detalhes sobre ativos incluídos nos inventários de ativos para permitir a gestão e o uso consistente dos ativos. Incluir informações necessárias sobre ativos para apoiar a estratégia do programa de cibersegurança ajuda a garantir que essas informações estejam disponíveis durante períodos de estresse operacional e não precisem ser coletadas em estado de crise. Por exemplo, a resposta e recuperação de um incidente de cibersegurança podem ser aceleradas se o inventário de ativos de informação fornecer a localização de backups para ativos de informação importantes para a entrega da <Instituição> (por exemplo, pontos de ajuste SCADA).

Além disso, a <Instituição> deve considerar os diferentes tipos de ativos que podem estar dentro do escopo da avaliação, como ativos virtualizados, ativos regulados, ativos em nuvem e ativos móveis.

E03-INFORMAÇÕES-01-F

O inventário de ativos de informação está completo (o inventário inclui todos os ativos dentro da <Instituição>)

Detalhamento:

Esta <Ação> amplia o escopo do inventário de ativos de informação. O nível de detalhe com que os ativos de informação são documentados no inventário deve ser determinado levando em consideração a importância e sensibilidade do ativo para a <Instituição>. Em muitos casos, pode ser benéfico consolidar tipos de ativos de informação em uma única entrada no inventário de ativos de informação. Por exemplo, ativos criados por funcionários residindo em estações de trabalho individuais (como arquivos ou bancos de dados) podem não justificar entradas separadas no inventário de ativos de informação, a menos que tenham valor especial ou crítico para a entrega da <Instituição>. A relação entre ativos e funções empresariais também deve ser incluída para permitir a priorização e o desenvolvimento de estratégias de proteção e sustentação. A implementação do inventário deve ser proporcional ao tamanho, complexidade e risco da <Instituição>. Por exemplo, para uma <Instituição> pequena e de baixa complexidade, uma planilha simples pode ser usada para o inventário. Para uma <Instituição> maior e mais complexa, métodos mais sofisticados, como uma aplicação dedicada de inventário de ativos, são apropriados.

E03-INFORMAÇÕES-01-G

O inventário de ativos de informação está atualizado, ou seja, é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema

Detalhamento:

O inventário de ativos de informação deve ser atualizado e mantido conforme os ativos mudam ao longo de seu ciclo de vida para garantir que o inventário seja completo e preciso. Garantir que o inventário de ativos de informação esteja atualizado pode envolver procedimentos de gestão de mudanças que exigem atualizações de inventário sempre que os ativos são significativamente alterados. a <Instituição> também pode realizar revisões de estoque, tanto periodicamente (como trimestral ou anualmente) quanto com base em eventos (como mudanças na estrutura organizacional, grandes mudanças em sistemas críticos e aquisição e consolidação de outro negócio).

E03-INFORMAÇÕES-01-H

Os ativos de informação são higienizados ou destruídos no final da vida útil usando técnicas adequadas às suas necessidades de cibersegurança

Detalhamento:

Nesta <Ação>, sanitização refere-se à remoção de dados sensíveis de um ativo em preparação para sua reutilização. Por exemplo, a higienização pode envolver remover informações específicas do cliente de uma apresentação de slides para que possam ser usadas novamente. Isso deve ser feito de forma a evitar a divulgação de informações a indivíduos não autorizados quando os bens forem reutilizados.

Por outro lado, destruição refere-se à remoção de dados para que não possam ser recuperados. Isso envolve remoção permanente (ou seja, exclusão de forma que torne a recuperação impossível, como apagamento criptográfico, desidentificação de informações pessoais identificáveis (PII) e destruição) de ativos de TI e ativos TO quando não são mais necessárias. a <Instituição> deve determinar quais ações de fim de vida são apropriadas para os ativos de informação e criar procedimentos para garantir conformidade com as diretrizes de retenção que determinam quando os ativos de informação devem

ser aposentados. Os procedimentos devem incluir todos os locais possíveis onde cópias das informações possam ser armazenadas, incluindo logs do sistema.

E03-INFORMAÇÕES-02

Implementar a segurança de dados

E03-INFORMAÇÕES-02-A

Os dados são destruídos ou removidos com segurança dos ativos de hardware de TI antes de sua realocação e no final de sua vida útil

Detalhamento:

Os dados são removidos permanentemente (ou seja, excluídos de forma impossível a recuperação de dados) dos ativos de TI e de TO antes de serem reutilizados ou liberados para descarte. A seleção das técnicas de remoção e destruição de dados deve estar proporcional às exigências de cibersegurança da <Instituição>. Técnicas de remoção de dados, incluindo limpeza, purga, apagamento criptográfico, desidentificação de informações pessoais identificáveis e destruição, impedem a divulgação de informações a indivíduos não autorizados quando tais mídias são reutilizadas. A destruição dos dados também pode ser alcançada por meio da destruição do suporte onde eles são armazenados (como a destruição física de um disco rígido). Ativos como dispositivos móveis que têm maior probabilidade de mudar de localização ou propriedade podem exigir atividades adicionais para garantir que os dados não sejam acessados por indivíduos não autorizados. Isso pode incluir criptografia total de disco em laptops ou remoção remota de dados para dispositivos móveis.

Além disso, considere ativos que podem estar fora do controle direto da <Instituição> para manutenção, máquinas virtuais inativas, backups de máquinas virtuais e snapshots de máquinas virtuais, que podem incluir dados sensíveis e devem ser destruídos quando não forem mais necessários.

E03-INFORMAÇÕES-02-B

Os dados são destruídos ou removidos com segurança dos ativos de software de TI antes da realocação e no final da vida útil

Detalhamento:

Os dados são removidos permanentemente (ou seja, excluídos de forma impossível a recuperação de dados) dos ativos de software de TI e de TO antes de serem reutilizados ou liberados para descarte. A seleção das técnicas de remoção e destruição de dados deve estar proporcional às exigências de cibersegurança da <Instituição>. Técnicas de remoção de dados, incluindo limpeza, purga, apagamento criptográfico, desidentificação de informações pessoais identificáveis e destruição, impedem a divulgação de informações a indivíduos não autorizados quando tais mídias são reutilizadas. A destruição dos dados também pode ser alcançada por meio da destruição do suporte onde eles são armazenados (como a destruição física de um disco rígido). Ativos como dispositivos móveis que têm maior probabilidade de mudar de localização ou propriedade podem exigir atividades adicionais para garantir que os dados não sejam acessados por indivíduos não autorizados. Isso pode incluir criptografia total de disco em laptops ou remoção remota de dados para dispositivos móveis.

Além disso, considere ativos que podem estar fora do controle direto da <Instituição> para manutenção, máquinas virtuais inativas, backups de máquinas virtuais e snapshots de máquinas virtuais, que podem incluir dados sensíveis e devem ser destruídos quando não forem mais necessários.

E03-INFORMAÇÕES-02-C

Os dados são destruídos ou removidos com segurança dos ativos de TO antes da realocação e no final da vida útil

Detalhamento:

Os dados são removidos permanentemente (ou seja, excluídos de forma impossível a recuperação de dados) dos ativos de TI e de TO antes destes serem reutilizados ou liberados para descarte. A seleção das técnicas de remoção e destruição de dados deve estar proporcional às exigências de cibersegurança da <Instituição>. Técnicas de remoção de dados, incluindo limpeza, purga, apagamento criptográfico, desidentificação de informações pessoais identificáveis e destruição, impedem a divulgação de informações a indivíduos não autorizados quando tais mídias são reutilizadas. A destruição dos dados também pode ser alcançada por meio da destruição do suporte onde eles são armazenados (como a destruição física de um disco rígido). Ativos como dispositivos móveis que têm maior probabilidade de mudar de localização ou propriedade podem exigir atividades adicionais para garantir que os dados não sejam acessados por indivíduos não autorizados. Isso pode incluir criptografia total de disco em laptops ou remoção remota de dados para dispositivos móveis.

Além disso, considere ativos que podem estar fora do controle direto da <Instituição> para manutenção, máquinas virtuais inativas, backups de máquinas virtuais e snapshots de máquinas virtuais, que podem incluir dados sensíveis e devem ser destruídos quando não forem mais necessários.

E03-INFORMAÇÕES-02-D

Os dados são destruídos ou removidos com segurança dos ativos de software de TI antes da realocação e no final da vida útil

Detalhamento:

Os dados são removidos permanentemente (ou seja, excluídos de forma impossível a recuperação de dados) dos ativos de software de TI e de TO antes destes serem reutilizados ou liberados para descarte. A seleção das técnicas de remoção e destruição de dados deve estar proporcional às exigências de cibersegurança da <Instituição>. Técnicas de remoção de dados, incluindo limpeza, purga, apagamento criptográfico, desidentificação de informações pessoais identificáveis e destruição, impedem a divulgação de informações a indivíduos não autorizados quando tais mídias são reutilizadas. A destruição dos dados também pode ser alcançada por meio da destruição do suporte onde eles são armazenados (como a destruição física de um disco rígido). Ativos como dispositivos móveis que têm maior probabilidade de mudar de localização ou propriedade podem exigir atividades adicionais para garantir que os dados não sejam acessados por indivíduos não autorizados. Isso pode incluir criptografia total de disco em laptops ou remoção remota de dados para dispositivos móveis.

Além disso, considere ativos que podem estar fora do controle direto da <Instituição> para manutenção, máquinas virtuais inativas, backups de máquinas virtuais e snapshots de máquinas virtuais, que podem incluir dados sensíveis e devem ser destruídos quando não forem mais necessários.

E03-INFORMAÇÕES-02-E

Dados sensíveis são protegidos em repouso

Detalhamento:

Técnicas de autenticação (por exemplo, gerenciamento de credenciais, certificados digitais, identificação biométrica, autenticação multifator), técnicas de autorização (por exemplo, mecanismos de controle de acesso) e técnicas de proteção (por exemplo, criptografia e mascaramento de dados) são

táticas arquitetônicas típicas para proteger dados sensíveis em repouso. Aplicar múltiplas técnicas não é necessário para implementar esta <Ação>. Os dados em repouso podem incluir dados armazenados em ativos virtualizados adormecidos.

E03-INFORMAÇÕES-02-F

Todos os dados em repouso são protegidos para categorias selecionadas de dados

Detalhamento:

As informações podem ser categorizadas (conforme referenciado no ATIVO-2c) de acordo com várias considerações de segurança, incluindo sensibilidade, valor, criticidade ou requisitos legais. Esta <Ação> estende as táticas arquitetônicas para dados em repouso mencionadas na ARQUITETURA-5a, como autenticação (por exemplo, gerenciamento de credenciais, certificados digitais, identificação biométrica, autenticação multifator), autorização (por exemplo, mecanismos de controle de acesso) e proteção (por exemplo, criptografia e mascaramento de dados). Táticas arquitetônicas de proteção de dados também podem incluir, por exemplo, o uso de uma camada de acesso seguro aos dados em vez de permitir acesso direto a armazenamentos de dados.

E03-INFORMAÇÕES-02-G

Todos os dados em trânsito são protegidos para categorias selecionadas de dados

Detalhamento:

Protocolos criptográficos e mascaramento de dados são exemplos de táticas arquitetônicas típicas para proteger dados sensíveis em trânsito e promover o compartilhamento seguro de dados. Dependendo da categoria de dados, proteções adicionais, como o uso de uma rede privada virtual, podem ser necessárias.

E03-INFORMAÇÕES-02-H

Controles criptográficos são implementados para dados em repouso e dados em trânsito para categorias de dados selecionadas

Detalhamento:

Esta <Ação> promove o estabelecimento e manutenção de controles criptográficos para proteção de dados em repouso ou em trânsito. Isso inclui a seleção, aposentadoria e substituição de controles criptográficos para acompanhar as mudanças tecnológicas (como computação quântica). Ela incorpora decisões de design e justificativas sobre o nível desejado de criptografia. Por exemplo, alguns algoritmos criptográficos têm desempenho melhor que outros, e por isso há concessões entre a força da criptografia e o desempenho do sistema e a facilidade de manutenção. Também há considerações de projeto para dados em repouso, como criptografia total de disco, criptografia baseada em arquivos e criptografia baseada em contêineres. Os dados em repouso podem incluir dados armazenados em ativos virtualizados adormecidos. O termo "categorias de dados selecionadas" é usado nesta <Ação> para significar que a <Instituição> deve selecionar explicitamente os tipos de dados que precisam ser criptografados durante o trânsito. Por exemplo, a <Instituição> pode optar por não criptografar sinais TO em uma rede isolada, mas pode exigir criptografia para todos os dados em trânsito em uma aplicação voltada para a web.

E03-INFORMAÇÕES-02-I

Controles para restringir a exfiltração de dados (por exemplo, ferramentas de prevenção de perda de dados) são implementados

Detalhamento:

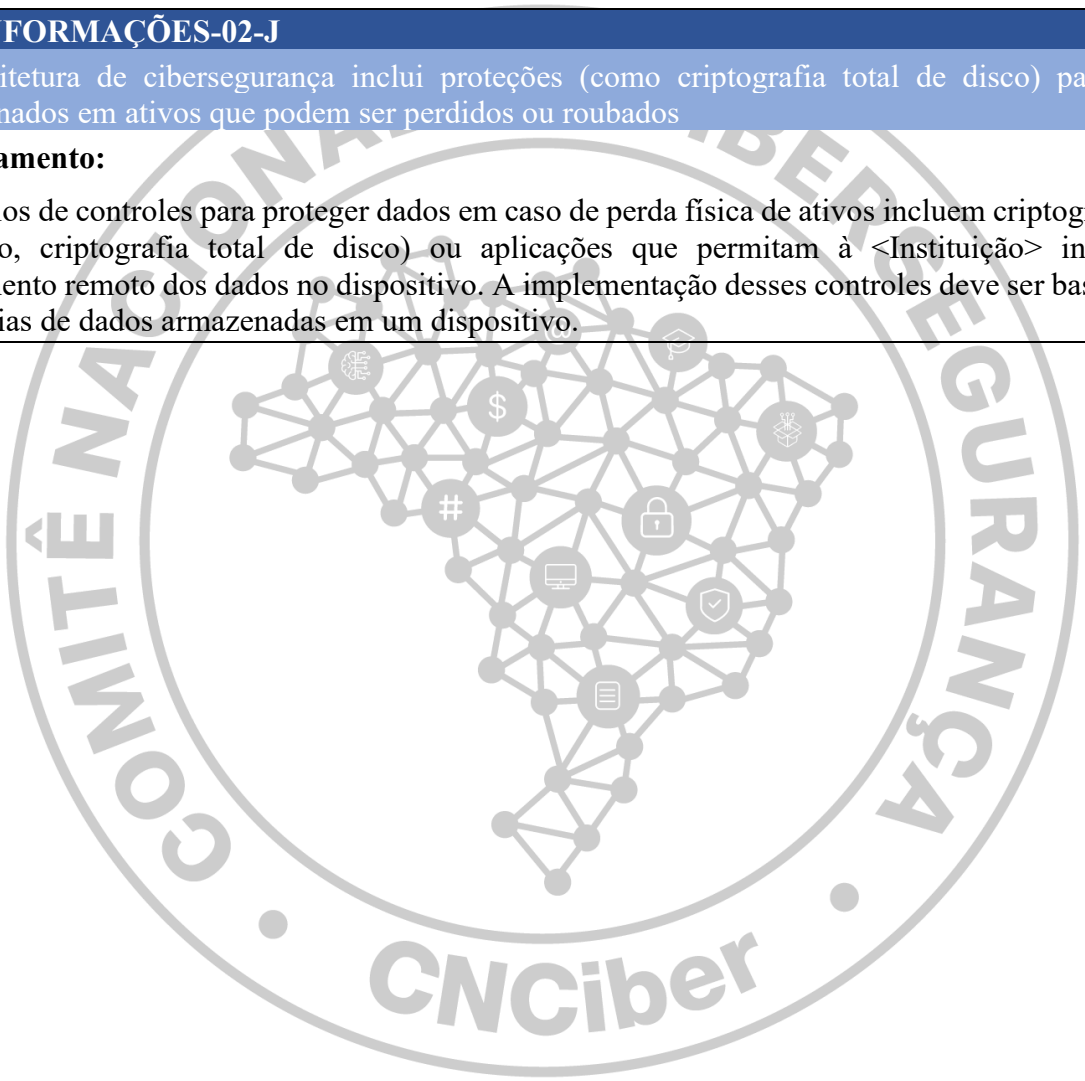
Exemplos de controles para restringir a exfiltração de dados incluem táticas arquitetônicas como autenticação e autorização, restrição de acesso remoto (incluindo o uso de serviços em nuvem) e monitoramento da atividade do usuário (por exemplo, para uploads de alto volume de dados para sistemas externos).

E03-INFORMAÇÕES-02-J

A arquitetura de cibersegurança inclui proteções (como criptografia total de disco) para dados armazenados em ativos que podem ser perdidos ou roubados

Detalhamento:

Exemplos de controles para proteger dados em caso de perda física de ativos incluem criptografia (por exemplo, criptografia total de disco) ou aplicações que permitam à <Instituição> iniciar um apagamento remoto dos dados no dispositivo. A implementação desses controles deve ser baseada nas categorias de dados armazenadas em um dispositivo.



E04-ACESSOS

Gerenciamento de identidade e acesso

Resumo:

Para os fins deste <Eixo>, o controle de acesso se aplica ao acesso lógico aos ativos usados na entrega da função, ao acesso físico aos ativos relevantes para a função e aos sistemas automatizados de controle de acesso (lógicos ou físicos) relevantes para a função. Práticas inadequadas de gerenciamento de acesso podem levar ao uso, divulgação, destruição ou modificação não autorizados, bem como exposição desnecessária a ciber-riscos.

Detalhamento:

O estabelecimento e a manutenção de identidades começam com o provisionamento e o desprovisionamento (remoção de identidades disponíveis quando não são mais necessárias) de identidades para entidades. As entidades podem incluir indivíduos (internos ou externos à <Instituição>), dispositivos, sistemas ou processos que requerem acesso a ativos. Em alguns casos, instituições podem precisar usar identidades compartilhadas. O gerenciamento de identidades compartilhadas pode exigir medidas compensatórias para garantir um nível adequado de segurança. A manutenção de identidades inclui a rastreabilidade (garantir que todas as identidades conhecidas sejam válidas) e o desprovisionamento.

O controle do acesso lógico e físico inclui determinar os requisitos de acesso, conceder acesso a ativos com base nesses requisitos e revogar o acesso quando ele não for mais necessário. Os requisitos de acesso lógico e físico estão associados a cada ativo (ou conjunto de ativos) dentro de uma determinada área e fornecem orientação para os tipos de entidades ou indivíduos autorizados a acessar o ativo, os limites de acesso permitido e, para acesso lógico, parâmetros de autenticação. Por exemplo, os requisitos de acesso lógico para um ativo específico podem permitir o acesso remoto por um fornecedor somente durante intervalos de manutenção especificados e planejados e também podem exigir autenticação multifator para esse acesso. Em níveis mais altos de maturidade, mais escrutínio é aplicado ao acesso concedido. O acesso lógico e físico é concedido somente após considerar o risco para a função, e revisões regulares de acesso são realizadas.

E04-ACESSOS-01

Estabelecer acessos e identidades

E04-ACESSOS-01-A

Identidades são provisionadas, para pessoal e outras entidades, como serviços e dispositivos que exigem acesso a ativos (note que isso não exclui identidades compartilhadas)

Detalhamento:

Provisão refere-se à criação ou registro de identidades. Isso envolve identificar a entidade e documentar atributos como papel e posição na <Instituição>.

O provisionamento é realizado para pessoas, dispositivos, sistemas e processos, sejam internos ou externos à <Instituição>. Assim, um fornecedor, agência ou parceiro comercial pode ser registrado como identidade pela <Instituição>, assim como um sistema ou processo de uma <Instituição> externa. Em alguns casos, a <Instituição> pode precisar usar identidades compartilhadas, como contas de grupo.

Uma boa <Ação> para provisionamento é o perfil de identidade. O perfil contém todas as informações relevantes necessárias para descrever os atributos, papéis e responsabilidades únicos da entidade

associada. O perfil de identidade geralmente é iniciado e aprovado pela unidade organizacional ou linha de negócios à qual a entidade pertence e onde podem ser tomadas decisões sobre o uso dos ativos organizacionais.

E04-ACESSOS-01-B

Identidades são desprovisionadas, quando não são mais necessárias

Detalhamento:

Quando uma pessoa, objeto ou entidade deixa de existir na <Instituição>, a identidade associada e todos os seus privilégios e restrições de acesso devem ser eliminados. A falha em desprovisionar uma identidade pode resultar em risco operacional significativo para uma <Instituição>, pois pode fornecer uma identidade à qual uma pessoa, objeto ou entidade não autorizada (e talvez desconhecida) possa se associar. Se isso ocorrer e seus privilégios de acesso não forem encerrados, a identidade pode ser roubada junto com todos os privilégios existentes.

E04-ACESSOS-01-C

Repositórios de identidade são revisados e atualizados periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e alterações na estrutura organizacional

Detalhamento:

A revisão periódica das identidades pode ajudar a <Instituição> a garantir que elas permaneçam viáveis e precisas. A revisão periódica deve ser realizada pela <Instituição> com a intenção de identificar identidades que não são mais válidas, que são duplicadas ou que mudaram materialmente, mas não foram detectadas pelo processo de gestão de mudanças. As revisões também podem revelar identidades com funções ou responsabilidades inválidas para as quais privilégios de acesso foram providenciados.

Identidades inválidas ou duplicadas podem resultar no uso e modificação não autorizados de informações, uso de sistemas e tecnologia, ou entrada e uso de instalações.

E04-ACESSOS-01-D

Identidades são desprovisionadas dentro de limites de tempo definidos pela <Instituição> quando não são mais necessárias

Detalhamento:

A desprovisionamento deve ocorrer como resultado do processo de mudança ou demissão de funcionários. a <Instituição> deve definir um requisito baseado em tempo dentro do qual a desprovisionação deve ser realizada. Por exemplo, após a término, a desprovisionamento deve ocorrer imediatamente; Para transições de funcionários para novas funções, o prazo pode ser maior.

Para que a desprovisionamento oportuno seja possível, deve haver um processo para que os departamentos de recursos humanos forneçam informações de rescisão para aqueles responsáveis pela manutenção dos repositórios de identidade da <Instituição>. A desaprovação também pode ser resultado de ações corretivas tomadas após uma revisão para remediar situações em que os limites de tempo não foram atingidos.

E04-ACESSOS-01-E

O uso de credenciais privilegiadas é limitado a processos para os quais elas são exigidas

Detalhamento:

Contas privilegiadas representam maior risco para ativos de TI. A <Instituição> deve controlar o uso de credenciais privilegiadas por meios administrativos, como uma política que restringe o uso de contas administrativas locais a tarefas obrigatórias e proíbe o uso de contas privilegiadas para funções do dia a dia. Alternativamente, uma <Instituição> pode implementar controles técnicos para restringir contas privilegiadas de acessar recursos que não exigem privilégios elevados.

E04-ACESSOS-01-F

Identidades e acessos são desativados com base em critérios estabelecidos

Detalhamento:

A aplicação da desprovisão de identidade pode reduzir o risco de uma conta inativa ser usada de forma inadequada ou sujeita a atividades maliciosas.

Critérios para desprovisionamento de acessos ou identidades devem incluir:

• Expiração do acesso ou identidade;

• Acesso desvinculado de uma identidade;

• Acesso violando política ou norma institucional;

• Inatividade do acesso: deve ser estabelecido pela <Instituição> de acordo com o risco potencial. Por exemplo, identidades temporárias fornecidas a empreiteiros podem ser devidamente desativadas após um período de 30 dias ou menos. uma <Instituição> pode implementar esse controle monitorando primeiro o carimbo de tempo do último logon ou outros atributos para identificar possíveis períodos de inatividade. Usando essas informações, identidades que estiveram inativas por um período definido podem ser identificadas, desativadas ou removidas caso não sejam mais necessárias.

• Afastamentos temporários.

A eficiência desta <Ação> pode ser melhorada ao desenvolver uma lista de contas que, por natureza, têm longos períodos de dormência, mas que são necessárias para atender aos requisitos operacionais.

Embora esta <Ação> possa ser aplicada por meios automatizados, é importante considerar cuidadosamente os impactos nas operações antes de implementar o desprovisionamento automático.

E04-ACESSOS-01-G

O processo de registro para a criação de uma identidade exige autorização formal

Detalhamento:

Uma identidade não pode simplesmente "existir" ou "ganhar acessos" sem um fluxo formalizado e documentado de governança.

É necessário que haja aprovações formais por pessoal ou papéis definidos pela <Instituição> (ex: gestores de área, proprietários dos dados ou RH) para qualquer solicitação de criação de contas de sistema.

A <Instituição> deve especificar detalhadamente os usuários autorizados, seus papéis (roles), grupos e as autorizações de acesso (privilégios) associadas a cada conta.

Um sistema só pode conceder o acesso real baseado em uma autorização de acesso válida, no uso pretendido do sistema e em outros atributos definidos pelo negócio.

Uma <Instituição> que opere em níveis moderados ou altos de Essencialidade é também necessário que a autorização formal e o ciclo de vida da identidade não dependam exclusivamente de processos manuais (como e-mails ou planilhas), exigindo-se o uso de mecanismos automatizados (sistemas de IGA - Identity Governance and Administration ou ferramentas de IAM) para criar, modificar, desativar e remover contas seguindo as regras de aprovação pré-estabelecidas.

E04-ACESSOS-01-H

Auditar ações de criação, modificação, desabilitação, remoção e provisionamento de direitos para uma identidade

Detalhamento:

A <Instituição> deve documentar e aprovar os procedimentos de gestão de contas, o que inclui definir como e onde os logs de criação, modificação, desabilitação, remoção e provisionamento de direitos para identidades serão armazenados e quem terá acesso a eles.

O sistema automatizado ou os administradores devem notificar o pessoal designado (como a equipe de segurança ou os donos dos dados) sempre que contas de sistema forem criadas, modificadas, desativadas ou removidas. Essa notificação é o primeiro passo para a visibilidade de auditoria em tempo real.

Nos níveis mais altos de maturidade a <Instituição> deve utilizar mecanismos automatizados para auditar ativamente a gestão de contas. Isso significa que o sistema deve:

• Registrar automaticamente quem solicitou a criação/modificação, quem aprovou, quando ocorreu e quais privilégios foram alterados.

• Sinalizar e reportar discrepâncias (por exemplo, se uma conta foi modificada sem um chamado de suporte correspondente ou sem a aprovação formal exigida.

Quando a criação ou modificação envolve uma conta com superpoderes (administradores de rede, root etc.), exige-se que esses eventos gerem alertas imediatos para o SOC (Security Operations Center) ou para os agentes de segurança, uma vez que a criação maliciosa de uma conta privilegiada é uma das principais técnicas de persistência de atacantes (Ransomware, APTs).

É importante que se monitore e audite se a criação ou modificação da identidade ocorreu de forma atípica. Por exemplo: uma nova conta de administrador criada às 3h da manhã de um domingo por um usuário que nunca realiza tarefas administrativas nesse horário.

Devem constar no Log de Auditoria ao menos as seguintes informações:

• Quem realizou a ação (ID do administrador ou sistema automatizado).

• O que foi alterado (quais permissões, grupos ou dados cadastrais mudaram).

• Quando a alteração foi feita (registro de data/hora sincronizado).

• Qual foi a justificativa/autorização (ID do chamado ou processo de aprovação).

E04-ACESSOS-01-I

Processo de criação de acessos e identidades satisfaz requisitos específicos

Detalhamento:

A <Instituição> deve estabelecer e seguir um processo estruturado para gerenciar o ciclo de vida das contas do sistema. Isso inclui a criação, modificação, desativação e exclusão de contas.

Para se criar uma identidade é obrigatório passar por um processo de verificação e comprovação de identidade (saber se a pessoa é quem diz ser). Além disso, a criação deve estar estritamente vinculada a uma pessoa física ou a um responsável técnico (no caso de contas de serviço), proibindo contas genéricas ou compartilhadas sem controle.

O processo de atribuição, modificação e revogação de direitos de acesso deve ser formalizado e controlado.

A concessão de acessos na criação da conta deve seguir estritamente duas regras de ouro:

• Princípio do Privilégio Mínimo (Least Privilege): O usuário só ganha o acesso estritamente necessário para sua função.

• Necessidade de Conhecer (Need-to-know): Só tem acesso à informação quem realmente precisa dela para trabalhar.

Nos níveis mais elevados de maturidade é necessária a aprovação explícita do proprietário da informação ou do ativo de informação antes que o acesso seja liberado.

A concessão e o uso de direitos de acesso privilegiados devem ser restringidos e controlados de forma extremamente rígida.

Na criação de acessos, as identidades administrativas não devem ser usadas para tarefas cotidianas (como ler e-mails ou navegar na internet). O processo de criação deve garantir que o administrador tenha duas contas separadas: uma conta comum para o dia a dia e uma conta privilegiada, usada apenas quando houver necessidade técnica comprovada e autorizada.Os seguintes procedimentos são realizados durante o processo de criação de um acesso ou identidade:

• Provisionamento dos atributos obrigatórios definidos pelo modelo RBAC;

• Aplicação imediata das políticas de segurança e de conformidade organizacional;

• Geração das credenciais iniciais de acesso e notificação ao responsável pela conta.

E04-ACESSOS-01-J

Acessos não correspondem a identificadores públicos associados a identidades

Detalhamento:

Esta <Ação> aborda uma técnica de segurança avançada (geralmente exigida para sistemas de alta criticidade/segurança) para mitigar ataques de engenharia social e força bruta.

A <Instituição> deve garantir que os identificadores de usuário atribuídos a sistemas internos não correspondam e não sejam publicamente associáveis a identificadores públicos das mesmas pessoas.

Identificadores públicos comuns são o e-mail corporativo padrão (nome.sobrenome@empresa.com), o número de CPF/CNPJ exposto em diários oficiais, o nome de usuário do LinkedIn ou o ID de crachá visível.

Não se recomenda o uso desses identificadores públicos como o username de login em sistemas críticos ou sensíveis. Em sistemas comuns, o nome de usuário é o e-mail. Para um atacante, isso significa que 50% da autenticação já foi descoberta (ele já tem o usuário, só falta a senha).

Ao não se permitir a utilização de identificadores públicos, o atacante não consegue adivinhar o ID de usuário interno, pois ele não segue o padrão do e-mail público ou do nome real da pessoa. Se o atacante tentar fazer um ataque de força bruta usando o e-mail da vítima em um sistema protegido por esse controle, o ataque falhará logo no preenchimento do usuário, antes mesmo de testar a senha.

Implementar esta <Ação> carreia desafios operacionais que exigem maturidade tecnológica:

• Cofres de Senhas e PAM (Privileged Access Management): ferramentas de PAM tornam-se obrigatórias. O usuário não precisa memorizar seu ID em cada ferramenta específica; ele faz login com sua identidade comum (MFA) no cofre, e o cofre injeta a credencial mascarada na sessão de forma transparente.

• Rastreabilidade Interna: o sistema de auditoria (SIEM) deve ser capaz de correlacionar logs. Se um ID específico fizer algo errado, o log registrará esse ID, mas os administradores de segurança devem conseguir rastrear instantaneamente que aquele ID pertence a determinada identidade real (usando tabelas de mapeamento estritamente protegidas).

E04-ACESSOS-02

Gerenciar a autenticação

E04-ACESSOS-02-A

Credenciais (como senhas, smartcards, certificados e chaves) são emitidas para pessoal e outras entidades que necessitam de acesso a ativos

Detalhamento:

Antes de conceder a funcionários e outras entidades acesso aos ativos organizacionais, a <Instituição> deve emitir credenciais para provar que o indivíduo que solicita acesso possui os privilégios necessários para acessar os ativos. As entidades podem incluir indivíduos (internos ou externos à <Instituição>), bem como dispositivos, sistemas ou processos que necessitam de acesso a ativos. Os privilégios associados a essas credenciais devem estar alinhados com os requisitos operacionais.

E04-ACESSOS-02-B

Restrições de força e reutilização de senha são definidas e aplicadas

Detalhamento:

Os requisitos de força de senha e reutilização podem não ser suportados por todos os recursos dentro da <Instituição>. Quando possível, esses requisitos podem ser informados por considerações de segurança e operacionais, tolerância ao risco da <Instituição>, perfil de ameaça da <Instituição> (AMEAÇA-2e), prioridade dos ativos, sensibilidade das informações ou outras considerações.

E04-ACESSOS-02-C

Credenciais mais fortes, autenticação multifator ou credenciais de uso único são necessárias para acesso de maior risco (como contas privilegiadas, contas de serviço, contas compartilhadas e acesso remoto)

Detalhamento:

Os requisitos para credenciais usadas para acessar os ativos da <Instituição> devem ser proporcionais ao risco associado aos ativos. Se uma <Instituição> usa uma matriz para determinar o impacto potencial e a prioridade dos riscos, ela pode desenvolver uma matriz complementar que especifica requisitos de credencial e autenticação para cada nível de impacto. Por exemplo, para acesso remoto a um sistema com riscos que podem resultar em impacto significativo (nível 4 de 5) e alta probabilidade de ocorrência (nível 4 de 5), um requisito correspondente pode estabelecer que o pessoal deve usar credenciais fortes, autenticação multifator ou credenciais de uso único. Em situações em que credenciais fortes (como MFA) podem ser justificadas, mas são impedidas por limitações tecnológicas,

considere implementar as configurações de autenticação mais fortes disponíveis e implementar controles compensatórios se considerado apropriado, com base em considerações de risco e operacionais.

A autenticação multifatorial (MFA) envolve o uso de dois ou mais fatores para alcançar a verificação de uma identidade. Os fatores incluem (1) algo que você sabe, como uma senha, (2) algo que você tem, como um token, (3) algo que você é, como uma impressão digital, ou (4) algo que indique que você está onde diz estar, como um token GPS. No exemplo acima, o pessoal pode ser obrigado a autenticar usando um ID de login, uma senha e um token.

Credenciais de uso único podem ser implementadas por meio de uma solução de gerenciamento de acesso privilegiado (PAM). As funcionalidades fornecidas por um PAM incluem acesso baseado em funções a credenciais privilegiadas, rotação automatizada de senhas, integração com MFA e auditoria do uso de credenciais privilegiadas.

Estes são exemplos específicos de acesso que podem apresentar maior risco para a <Instituição> :

• Contas privilegiadas

• Contas de serviço

• Contas compartilhadas (O uso dessas contas deve ser desencorajado em geral, mas não é possível em certos ativos legados de TI, onde controles adicionais são apropriados, como credenciais mais fortes como mencionado nesta <Ação>, controles físicos de acesso fortes, entre outros.)

• Acesso remoto

• Contas administrativas

• Acesso emergencial

• Acesso a ativos sensíveis

• Acesso a sistemas de gestão de ativos em nuvem ou virtuais

• Contas de gerenciamento de chaves criptográficas

• Contas de backup

(Note que, à medida que são estabelecidos requisitos para credenciais mais fortes ou multifatoriais para mais desses tipos de acesso, mais alto avança a <Instituição> no espectro de maturidade.)

Além disso, é importante notar que a palavra risco está sendo usada nesta <Ação> no sentido geral e não se destina a se referir a riscos específicos identificados no <Eixo> de Gestão de Riscos da metodologia. No entanto, a <Instituição> deve considerar o acesso aos ativos de TI e os controles aplicados a esse acesso durante a identificação, análise e resposta de riscos discutidas no <Eixo> de Gestão de Riscos.

E04-ACESSOS-02-D

A autenticação multifator é necessária para todos os acessos, sempre que viável

Detalhamento:

A autenticação multifator pode não ser suportada por todos os ativos dentro da <Instituição>. Sempre que possível, controles de autenticação mais rigorosos, como autenticação multifator, reduzem o risco de uso indevido da conta resultante de credenciais comprometidas. Quando a autenticação multifatorial não é viável, a <Instituição> pode considerar implementar controles de mitigação dependendo de seu apetite por risco, ambiente de ameaça e necessidades operacionais.

E04-ACESSOS-03

Controlar o acesso lógico

E04-ACESSOS-03-A

Controles lógicos de acesso são implementados

Detalhamento:

Os controles de acesso são um elemento-chave da proteção oferecida aos ativos. Privilégios e restrições de acesso descrevem o nível e a extensão de acesso fornecidos às identidades. Os privilégios de acesso devem ser proporcionais aos diversos papéis representados por uma identidade.

E04-ACESSOS-03-B

Privilégios de acesso lógico são revogados quando não são mais necessários

Detalhamento:

Proprietários e custodiantes de ativos são responsáveis por revogar privilégios de acesso lógico quando não são mais necessários, como na demissão ou transição de um funcionário para um novo cargo. Geralmente, os funcionários devem manter o conjunto mínimo de privilégios necessários para desempenhar suas responsabilidades designadas. Revogar o acesso lógico que não é mais necessário ajuda a evitar a agregação de privilégios de acesso.

E04-ACESSOS-03-C

Requisitos lógicos de acesso são estabelecidos e mantidos (por exemplo, regras para quais tipos de entidades podem acessar um ativo, limites de acesso permitido, restrições de acesso remoto, parâmetros de autenticação)

Detalhamento:

É responsabilidade do proprietário do ativo garantir que os requisitos para proteger e manter ativos sejam definidos para ativos sob seu controle, incluindo requisitos para controle do acesso lógico (por exemplo, regras para quais tipos de entidades podem acessar um ativo, limites de acesso permitido, restrições de acesso remoto e parâmetros de autenticação). Por exemplo, os requisitos lógicos de acesso para um ativo específico podem permitir acesso remoto por um fornecedor apenas durante intervalos de manutenção especificados e pré-planejados e podem exigir autenticação multifator para esse acesso. Como outro exemplo, pode ser apropriado aplicar controles lógicos de acesso adicionais (como revisão por pares) a ativos de alta prioridade.

Existem vários modelos para controle de acesso, como controle de acesso discricionário (DAC), controle de acesso obrigatório (MAC), controle de acesso baseado em funções (RBAC), controle de acesso baseado em políticas (PBAC) e controle de acesso baseado em atributos (ABAC). A seleção de um modelo de controle de acesso variará com base em vários fatores, como o ambiente operacional e a viabilidade da implementação. Por exemplo, uma <Instituição> pode optar por implementar um modelo de controle de acesso suportado pela infraestrutura atual, como o RBAC, e planejar a implementação futura de um modelo mais avançado, como o ABAC, como parte da aquisição de uma nova infraestrutura que suporte capacidades adicionais de controle de acesso.

Modelos avançados de segurança, como o Zero Trust, também podem orientar o desenvolvimento dos requisitos de acesso. Por exemplo, a implementação dos princípios de Zero Trust pode incluir a capacidade de coletar e usar informações adicionais (como informações comportamentais,

informações de geolocalização, inteligência de ameaças e outras informações contextuais) como parte da aplicação da política de acesso.

E04-ACESSOS-03-D

Os requisitos lógicos de acesso incorporam o princípio do privilégio mínimo

Detalhamento:

O princípio do privilégio mínimo é um requisito de segurança que estabelece limitações para usuários autorizados apenas aos privilégios que eles precisam para executar tarefas atribuídas de acordo com suas responsabilidades e funções e nada mais. A <Instituição> empregam o princípio do privilégio mínimo ao considerar a atribuição de direitos de acesso e controles para funções e sistemas específicos (incluindo funções, portas, protocolos e serviços específicos). O princípio do menor privilégio também se aplica aos processos do sistema de informação, garantindo que os processos operem em níveis de privilégio não superiores ao necessário para cumprir as missões e/ou funções organizacionais exigidas. A <Instituição> consideram o princípio do menor privilégio na criação de processos, funções e contas de sistemas de informação adicionais, conforme necessário. A <Instituição> também aplicam o princípio do menor privilégio ao projeto, desenvolvimento, implementação e operação de sistemas de TI. A aplicação do princípio do menor privilégio é uma consideração importante para a implementação dos princípios do Zero Trust.

E04-ACESSOS-03-E

Os requisitos lógicos de acesso incorporam o princípio da separação de funções

Detalhamento:

Esse princípio deve ser incluído nos requisitos de acesso para evitar ou reduzir o impacto potencial de erros ou atividades maliciosas e para prevenir fraudes potenciais. Por exemplo, a pessoa que solicita acesso não deve ser também a pessoa que concede acesso, e a pessoa que solicita acesso deve receber apenas o conjunto mínimo de privilégios necessários para desempenhar as responsabilidades atribuídas. Como mencionado em outras partes do modelo, é importante considerar privilégios de acesso para dispositivos, sistemas e processos que exigem acesso a ativos e como a separação deve ser aplicada. Por exemplo, sistemas que desempenham funções críticas de segurança podem exigir escrutínio adicional sobre quais pessoas ou entidades podem acessá-los, incluindo sistemas de controle de processos que eles protegem.

E04-ACESSOS-03-F

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

Detalhamento:

Privilégios para acesso lógico a um ativo são atribuídos e aprovados por proprietários de ativos, custodiantes ou delegados autorizados com base no papel da pessoa, objeto ou entidade que solicita acesso. O proprietário ou custodiante do ativo é responsável por conceder privilégios lógicos de acesso com base no papel da identidade e nos requisitos de cibersegurança do ativo. Proprietários e custodiantes de ativos devem estar cientes de quais identidades específicas exigem acesso aos seus ativos e validar essa exigência em relação aos requisitos de negócios e cibersegurança antes de conceder aprovação.

E04-ACESSOS-03-G

Privilégios lógicos de acesso que apresentam maior risco para a <Instituição> recebem escrutínio e monitoramento adicionais

Detalhamento:

Acesso privilegiado, contas de serviço, contas compartilhadas e acesso remoto devem estar sujeitos a um controle mais rigoroso do que o acesso rotineiro de usuários. Um escrutínio adicional pode exigir que as solicitações de acesso sejam aprovadas por mais de uma pessoa ou por um indivíduo com um nível de autoridade superior às solicitações de acesso de usuários padrão. Monitoramento adicional pode envolver o registro do uso de privilégios elevados. Por exemplo, em uma <Instituição> madura, o acesso privilegiado a contas compartilhadas pode ser implementado por meio de credenciais provisionadas que são válidas apenas pelo tempo necessário para realizar uma alteração aprovada.

Além disso, a equipe pode ser monitorada por meio de circuito fechado de televisão e capturas de tela enquanto essas credenciais estiverem em uso.

Estes são exemplos específicos de acesso que podem apresentar maior risco para a <Instituição> :

• Contas privilegiadas

• Contas de serviço

• Contas compartilhadas

• Acesso remoto

• Contas administrativas

• Acesso de emergência

• Acesso a ativos sensíveis

• Acesso a sistemas de gestão de ativos em nuvem ou virtuais

• Contas de gerenciamento de chaves criptográficas

• Contas de backup

Além disso, é importante notar que a palavra risco está sendo usada nesta <Ação> no sentido geral da palavra e não se destina a nenhum riscos específicos identificados no <Eixo> de Gestão de Riscos da metodologia. No entanto, a <Instituição> deve considerar o acesso a ativos de TI e a suficiência dos controles para gerenciar o acesso como potenciais fontes de risco que devem ser consideradas nas atividades de identificação, análise e resposta de risco discutidas no <Eixo> de Gestão de Riscos.

E04-ACESSOS-03-H

Privilégios lógicos de acesso são revisados e atualizados periodicamente para garantir conformidade com os requisitos de acesso e de acordo com gatilhos definidos, como mudanças na estrutura organizacional e após qualquer elevação temporária de privilégios

Detalhamento:

Mudanças constantes no ambiente operacional criam a possibilidade de que, a qualquer momento, o nível atual de acesso lógico fornecido a pessoas, objetos e entidades (conforme refletido nos privilégios de acesso) possa não corresponder ao nível de necessidade baseado nos requisitos lógicos atuais de acesso. a <Instituição> deve definir um cronograma para revisão regular dos privilégios de acesso lógico, a fim de garantir que os requisitos estabelecidos para seus ativos estejam sendo implementados

por meio da atribuição adequada de privilégios lógicos de acesso e implementação dos respectivos controles lógicos de acesso.

Certos eventos temporários, como projetos ou respostas a incidentes, podem exigir a concessão de acesso lógico privilegiado baseado em situações. Uma revisão lógica de acesso deve ser um passo necessário no processo de encerramento desses eventos.

E04-ACESSOS-03-I

Tentativas anômalas de acesso lógico são monitoradas como indicadores de eventos de cibersegurança

Detalhamento:

O monitoramento é feito em tentativas lógicas de acesso, e quaisquer anomalias detectadas (como uma tentativa de login com um nome de usuário que não existe no sistema) são marcadas como exigindo revisão adicional para determinar se são indicadores de eventos de cibersegurança (e não erro do usuário, por exemplo).

E04-ACESSOS-03-J

Existe mecanismo resistente a ataques de força bruta

Detalhamento:

A <Instituição> deve empregar técnicas que impeçam um atacante de realizar testes massivos e sucessivos de credenciais.

Os principais mecanismos a serem implementados consistem em:

• Bloqueio Temporário do Acesso: impede-se novas tentativas de login para aquela conta ou a partir daquele endereço IP após um número predefinido de falhas consecutivas (ex: bloquear por 30 minutos após 5 erros).

• Atraso Progressivo (Throttling): aumenta-se artificialmente o tempo de resposta do sistema a cada tentativa errada (o primeiro erro responde em 1 segundo, o quinto erro demora 15 segundos para responder). Isso inviabiliza ataques de força bruta baseados em velocidade.

• Controles de Desafio Humano: introduzem-se validações de Turing (como CAPTCHAs) para garantir que a tentativa de login está partindo de um humano, quebrando a automação de ferramentas de ataque como o Hydra ou Burp Suite.

• Redefinição Forçada de Senha: determina-se que, se um limite crítico de tentativas incorretas for atingido, o sistema pode forçar o bloqueio definitivo da conta até que uma redefinição de senha seja feita através de um canal secundário verificado (como e-mail cadastrado ou validação via Service Desk).

Idealmente, recomenda-se o uso de MFA e Autenticação Adaptativa:

• Uso Obrigatório de MFA (Multi-Factor Authentication): mesmo que um ataque de força bruta descubra a senha por pura sorte, o atacante será bloqueado no segundo fator (token, SMS, biometria).

• Autenticação Baseada em Risco (Adaptativa): o sistema deve analisar padrões. Se houver tentativas vindas de localizações geográficas impossíveis ou dispositivos desconhecidos, o mecanismo deve exigir fatores de autenticação adicionais ou bloquear o login preventivamente, mesmo se a senha digitada estiver correta.

E04-ACESSOS-03-K

Existe uma lista de restrição de senhas

Detalhamento:

As melhores práticas internacionais recentes abandonaram a antiga lógica de forçar os usuários a criarem senhas complexas e cheias de regras (como misturar maiúsculas, minúsculas e símbolos, o que costuma gerar senhas previsíveis como P@ssword123).

A abordagem moderna foca em proibir o uso de senhas fracas ou vazadas, o que é feito por meio de uma lista de restrição de senhas (Password Blacklist), e trata do ciclo de vida e da aplicação dessa lista de restrição:

• O sistema deve manter uma lista de senhas comumente usadas, previsíveis ou comprovadamente já comprometidas (vazadas na internet).

• Essa lista deve incluir palavras de dicionário, sequências numéricas/letras (ex: 123456), o próprio nome do usuário, variações do nome da <Instituição>/sistema, datas comemorativas da <Instituição>, nomes de produtos, serviços ou departamentos internos ou senhas clássicas de mercado.

• O sistema deve validar ativamente, no exato momento em que o usuário cria ou altera sua senha, se o que ele digitou consta na lista de restrição. Se constar, a senha deve ser rejeitada imediatamente, forçando o usuário a escolher outra.

• Enquanto a senha está trafegando (inclusive durante o processo de checagem contra a lista de restrição), ela seja enviada exclusivamente através de canais criptografados protegidos (como TLS), para que a nova credencial não seja interceptada na rede.

A relação com a lista: Ele exige que A <Instituição> definam regras rígidas para desencorajar o uso de senhas fracas. A diretriz de implementação sugere que o sistema use ferramentas automatizadas para impedir a escolha de senhas óbvias, adotando listas de termos banidos (como datas comemorativas da empresa, nomes de produtos internos ou senhas clássicas de mercado).

E04-ACESSOS-03-L

O feedback de autenticação obscurece informações relevantes para um atacante

Detalhamento:

O feedback do resultado da autenticação evita fornecer informação potencialmente explorável por agentes de ameaça. O projeto da tela de login deve impedir que o atacante obtenha pistas estruturais, a exemplo de:

• Minimizar a Assistência em Caso de Falha: o sistema nunca deve dizer qual parte do login está errada. Mensagens como "Usuário correto, mas senha incorreta" são proibidas. A resposta deve ser genérica: "Usuário ou senha incorretos".

• Ocultação de Dados Sensíveis: mascarar as senhas na tela enquanto são digitadas (usando asteriscos ***) para evitar ataques de observação (shoulder surfing).

• Não Validar de Forma Fragmentada: O sistema só deve processar a validação após todos os dados estarem preenchidos (evitando técnicas de enumeração de usuários por tempo de resposta do servidor).

E04-ACESSOS-03-M

Quando de uma autenticação com sucesso o usuário é informado do último login malsucedido e do último bem-sucedido

Detalhamento:

Ao efetuar um login com sucesso o usuário é informado da data e hora do último login bem-sucedido e o último login malsucedido. Isso transforma o próprio usuário num agente de monitoramento da segurança do sistema.

E04-ACESSOS-03-N

A lista de restrição de senhas é atualizada

Detalhamento:

A lista de restrição de senhas é atualizada:

• Em uma frequência definida pela <Instituição>; ou

• Imediatamente caso haja suspeita de vazamento de credenciais na própria empresa.

E04-ACESSOS-03-O

Restrições de acesso remoto

Detalhamento:

A <Instituição> deve adotar uma governança sobre canais remotos, determinando as seguintes restrições:

• Definição de Tipos Permitidos: a <Instituição> deve documentar explicitamente quais tipos de acesso remoto são permitidos (ex: VPN corporativa, portais web protegidos por TLS, VDI/Desktop Virtual) e quais são estritamente proibidos (ex: conexões RDP diretas para a internet ou protocolos sem criptografia como Telnet).

• Autorização Prévia Específica: nenhum usuário pode ter acesso remoto habilitado "por padrão". Cada liberação exige uma justificativa de negócio e uma autorização formal antes que a conexão seja permitida.

• Controle de Rotas de Conexão: exige que a <Instituição> monitore e restrinja os pontos de entrada na rede. Todo o tráfego remoto deve passar por pontos de acesso controlados e autorizados (como firewalls de borda e gateways de VPN centralizados), impedindo que usuários criem "atalhos" ou conexões diretas aos servidores.

• Criptografia em Trânsito: todo e qualquer tráfego de acesso remoto deve ser criptografado utilizando protocolos robustos para proteger a confidencialidade e a integridade dos dados enquanto eles viajam pela internet pública.

Para cenários de maior maturidade considera-se "camadas" que restringem mais severamente a liberdade do usuário remoto para proteger o ecossistema interno:

• Monitoramento e Controle Automatizados (Automated Monitoring and Control): exige o uso de ferramentas automatizadas para monitorar as conexões remotas em tempo real. O sistema deve ser capaz de registrar a origem, o destino e as ações do usuário, gerando alertas ou derrubando a sessão automaticamente caso um comportamento suspeito ou violação de política seja detectado.

• Proteção de Desconexão (Disconnect / Re-authentication): determina que o sistema deve encerrar a conexão remota após um período específico de inatividade e exigir que o usuário passe por um processo completo de reautenticação para restabelecer o acesso, impedindo que uma sessão remota fique aberta indefinidamente.

• Restrições Baseadas em Recursos e Protocolos (Managed Access Control Points): exige que os usuários remotos não tenham acesso à rede interna como um todo. Em vez disso, o acesso deve ser roteado exclusivamente para portais gerenciados (como proxies reversos ou arquiteturas ZTNA - Zero Trust Network Access), onde o usuário só enxerga as aplicações específicas para as quais foi autorizado.

• Restrição de Execução de Comandos Privilegiados (Privileged Commands): uma das restrições mais críticas: usuários conectados remotamente não devem ter permissão para executar comandos administrativos ou privilegiados (como alterar configurações de firewall ou formatar servidores), a menos que a conexão remota seja feita de um ambiente altamente controlado e utilizando métodos de autenticação adicionais (MFA robusto e gateways de PAM).

• Inspeção de Postura do Dispositivo (Device Sanity / Posture Check): determina que o sistema só deve permitir a conexão remota se o dispositivo do usuário (mesmo que seja um computador corporativo) passar por uma validação de conformidade no momento do login. O sistema inspeciona se:

- O antivírus está ativo e atualizado.
- O sistema operacional possui os patches de segurança mais recentes.
- O firewall local está ligado.

Se o dispositivo falhar na inspeção, o acesso remoto é bloqueado ou colocado em quarentena, independentemente de o usuário ter digitado a senha e o MFA corretos.

E04-ACESSOS-03-P

Desabilitação de acesso por "violação de conduta"

Detalhamento:

Esta é uma <Ação> que lida cirurgicamente com situações de violação de conduta, riscos internos iminentes ou desligamentos hostis, determinando uma ação imediata e coordenada entre a equipe de segurança da informação, os recursos humanos e a gestão organizacional.

A <Instituição> deve desativar as contas de sistema de indivíduos identificados como de alto risco imediatamente após a determinação do risco.

Quando aplicado a um cenário de violação de conduta (como fraude, roubo de dados, assédio, sabotagem ou violação grave das políticas da empresa), deve-se alterar o protocolo padrão de desligamento de funcionários de "operacional/burocrático" para um estado de resposta a incidentes.

Para tanto, a <Instituição> não pode depender dos fluxos tradicionais de RH, que costumam levar dias. Uma implementação adequada deve considerar:

• Gatilho Imediato (Immediate Trigger): assim que uma violação grave de conduta é confirmada (ou quando um indivíduo é formalmente classificado como "ameaça interna" ou insider threat), a equipe de segurança deve ter a autoridade legal e técnica para cortar os acessos. O tempo de resposta aqui é medido em minutos, não em horas.

• Desativação em Massa e Centralizada: a desativação não se resume a bloquear o e-mail corporativo. O sistema (geralmente apoiado por ferramentas de IAM/IGA e automações de SOAR) deve propagar o bloqueio instantaneamente para:

- Contas de rede local (Active Directory / Entra ID).
- Sistemas de nuvem (SaaS, ERPs, CRMs).
- Acessos físicos às dependências da empresa (crachás e biometria).

• Conexões ativas de VPN ou ferramentas de acesso remoto (derrubando as sessões vigentes no ato).

• Preservação de Evidências (Conexão com Forense): em casos de violação de conduta, a conta deve ser desativada/bloqueada, e não excluída. Apagar a conta pode destruir logs de auditoria cruciais, caixas de e-mail e históricos de arquivos que servirão como provas legais em processos trabalhistas, cíveis ou criminais contra o indivíduo.

E04-ACESSOS-04

Controlar o acesso físico

E04-ACESSOS-04-A

Controles físicos de acesso (como cercas, eclusas e sinalização) são implementados

Detalhamento:

Para fins do modelo, esses controles são destinados à proteção de ativos de TI, TO e informações (por exemplo, bloqueios que controlam a entrada de um data center)Além disso, é importante considerar que a eficácia de alguns tipos de controles físicos de acesso, como chaves e crachás, pode ser significativamente impactada pela forma como são gerenciados e protegidos.

E04-ACESSOS-04-B

Privilégios de acesso físico são revogados quando não são mais necessários

Detalhamento:

Proprietários e custodiantes de ativos são responsáveis por revogar privilégios de acesso físico quando eles não são mais necessários por quem (ou o que quer que seja) a quem foram designados, como após a demissão ou a transição para um novo cargo do funcionário. Geralmente, os funcionários devem manter o conjunto mínimo de privilégios necessários para desempenhar suas responsabilidades designadas. Revogar o acesso físico que não é mais necessário ajuda a evitar a agregação de privilégios de acesso.

E04-ACESSOS-04-C

Os registros físicos de acesso são mantidos

Detalhamento:

É responsabilidade do proprietário do ativo garantir que o registro do acesso físico atenda aos requisitos para proteger e manter o ativo sob controle do proprietário. O registro pode ser realizado por meios manuais, como um registro em papel, ou por meios automatizados, como dados coletados por sistemas físicos de controle de acesso.

E04-ACESSOS-04-D

Os requisitos de acesso físico são estabelecidos e mantidos (por exemplo, regras sobre quem pode acessar um ativo, como o acesso é concedido, limites de acesso permitido)

Detalhamento:

É responsabilidade do proprietário do ativo garantir que os requisitos para proteção e manutenção dos ativos sejam definidos para os ativos sob controle do proprietário, incluindo os requisitos para controle do acesso físico. Por exemplo, requisitos de acesso físico para visitas de fornecedores a data centers

podem exigir a emissão de um crachá temporário, acesso acompanhado e um membro da equipe monitorando as atividades do visitante.

E04-ACESSOS-04-E

Os requisitos de acesso físico incorporam o princípio do menor privilégio

Detalhamento:

O princípio do privilégio mínimo deve ser incorporado sempre que possível ao determinar requisitos de acesso físico para evitar ou reduzir o impacto potencial de erros ou atividades maliciosas. Por exemplo, a pessoa que solicita acesso a uma instalação deve ter acesso apenas às áreas necessárias para cumprir as responsabilidades designadas.

E04-ACESSOS-04-F

Os requisitos de acesso físico incorporam o princípio da separação de funções

Detalhamento:

O princípio da separação de funções deve ser incorporado sempre que possível ao determinar requisitos de acesso físico para evitar ou reduzir o impacto potencial de erros ou atividades maliciosas. Por exemplo, um funcionário pode ter privilégios físicos de acesso para entrar em uma instalação, mas pode não ter acesso a um armário de servidores.

E04-ACESSOS-04-G

Solicitações de acesso físico são analisadas e aprovadas pelo proprietário do ativo

Detalhamento:

Existe um procedimento pelo qual proprietários de ativos, custodiantes ou delegados autorizados revisam e aprovam pedidos de ativos pelos quais são responsáveis. Proprietários e custodiantes de ativos devem estar cientes de quais identidades exigem acesso aos seus ativos e ser capazes de validar a exigência em relação aos requisitos de negócios e cibersegurança antes de conceder a aprovação.

E04-ACESSOS-04-H

Privilégios de acesso físico que apresentam maior risco para a <Instituição> recebem escrutínio e monitoramento adicionais

Detalhamento:

Instalações ou áreas onde ativos que apresentam maior risco para a <Instituição> podem ter controles físicos de acesso adicionais ou mais rigorosos. Uma análise adicional pode significar que os pedidos de acesso são aprovados por mais de uma pessoa ou por um indivíduo com um nível de autoridade superior aos pedidos de acesso padrão. Monitoramento adicional pode envolver requisitos adicionais de registro de acesso, vigilância adicional do ambiente, requisitos adicionais de distintivos e acompanhamento para visitantes. Isso pode ser implementado por meio de um fator de acesso adicional, registro adicional ou monitoramento ativo por seguranças. Por exemplo, uma <Instituição> pode ter um sistema geral de insígnia para acesso à instalação, mas também exigir que um PIN seja inserido para acesso físico a uma parte da instalação.

Além disso, é importante notar que a palavra risco está sendo usada nesta <Ação> no sentido geral e não se destina a se referir a riscos específicos identificados no <Eixo> de Gestão de Riscos da

metodologia. No entanto, a <Instituição> deve considerar o acesso a ativos de TI e a suficiência dos controles para gerenciar o acesso como potenciais fontes de risco que devem ser consideradas nas atividades de identificação, análise e resposta de risco discutidas no <Eixo> de Gestão de Riscos.

E04-ACESSOS-04-I

Os privilégios de acesso físico são revisados e atualizados

Detalhamento:

Mudanças constantes no ambiente operacional criam a possibilidade de que, a qualquer momento, o nível atual de acesso físico fornecido às pessoas (conforme refletido nos privilégios de acesso) possa não corresponder ao nível de necessidade baseado nos requisitos atuais de acesso físico. a <Instituição> deve definir um cronograma para revisão regular dos privilégios de acesso físico, a fim de garantir que os requisitos estabelecidos para seus ativos estejam sendo implementados por meio da atribuição adequada de privilégios de acesso físico e implementação dos controles físicos correspondentes.

Certos eventos temporários, como projetos ou respostas a incidentes, podem exigir a concessão de acesso físico privilegiado baseado em situações. Uma revisão de acesso físico deve ser uma etapa necessária no processo de encerramento desses eventos.

E04-ACESSOS-04-J

O acesso físico é monitorado para identificar possíveis eventos de cibersegurança

Detalhamento:

O monitoramento é feito em tentativas físicas de acesso, e quaisquer anomalias detectadas (como tentativas de acesso não aprovadas) são marcadas como necessitando de revisão adicional para determinar se são indicadores de eventos de cibersegurança (em vez de um erro, por exemplo).

E05-AMEAÇAS

Gerenciamento de ameaças e vulnerabilidades

Resumo:

Uma ciberameaça é qualquer circunstância ou evento com potencial para impactar negativamente as operações institucionais (incluindo missão, funções, imagem ou reputação), recursos ou outras instituições por meio de infraestrutura de TI, TO ou comunicações, por meio, por exemplo, de acesso não autorizado, destruição, divulgação ou modificação de informações, ou negação de serviço. Isso inclui agentes sem a intenção de causar impacto adverso (por exemplo, em decorrência de erros internos).

Uma vulnerabilidade de cibersegurança é uma fraqueza ou falha em sistemas ou dispositivos de TI, TO ou comunicações, procedimentos ou controles internos que podem ser explorados por uma ameaça.

Detalhamento:

A identificação e resposta a ameaças começa com a coleta de informações úteis sobre ameaças de fontes confiáveis, interpretando essas informações no contexto da <Instituição> e função e respondendo a ameaças que têm os meios, o motivo e a oportunidade de afetar a prestação de serviços. Um perfil de ameaça inclui a caracterização da provável intenção, capacidade e alvo de ameaças à função. O perfil de ameaça pode ser usado para orientar a identificação de ameaças específicas, o processo de análise de risco descrito no <Eixo> Gerenciamento de Riscos e a construção do status operacional e cibernético descrito no <Eixo> Consciência Situacional.

A redução de vulnerabilidades de cibersegurança começa com a coleta e análise de informações de vulnerabilidade. A descoberta de vulnerabilidades pode ser realizada usando ferramentas de verificação automática, testes de penetração de rede, exercícios de cibersegurança e auditorias. A análise de vulnerabilidade deve considerar o impacto local da vulnerabilidade (o efeito potencial da vulnerabilidade no ativo exposto), bem como a importância do ativo para a entrega da função. As vulnerabilidades podem ser abordadas implementando controles de mitigação, monitorando o status da ameaça, aplicando patches de cibersegurança, substituindo equipamentos desatualizados ou realizando outras <Ações>.

E05-AMEAÇAS-01

Reduzir as vulnerabilidades de cibersegurança

E05-AMEAÇAS-01-A

Fontes de informação para apoiar a descoberta de vulnerabilidades em cibersegurança são identificadas

Detalhamento:

Informações sobre vulnerabilidades potenciais estão disponíveis em uma ampla variedade de fontes internas e externas, como CISA, ISACs apropriados, associações industriais, fornecedores, briefings federais e avaliações internas. Fontes internas normalmente fornecem informações sobre vulnerabilidades únicas para a <Instituição> e que abrangem todos os tipos de ativos. Essas fontes podem fornecer informações sobre vulnerabilidades que a <Instituição> observou ou que foram exploradas, resultando em interrupções na <Instituição>. Fontes externas ou públicas normalmente fornecem informações focadas em tecnologias comuns utilizadas por uma ampla gama de organizações.

Vulnerabilidades no sentido tradicional incluem bugs de software, erros de omissão, construção ruim de código, má configuração ou falhas de processamento. No entanto, outras exposições a riscos podem

criar vulnerabilidades que devem ser identificadas, processadas e respondidas de forma semelhante às vulnerabilidades que, por exemplo, são relatadas por fornecedores de software ou incluídas em catálogos de vulnerabilidades. Esses tipos de vulnerabilidades podem incluir baixo desempenho de processos, ameaças internas e descobertas de auditorias internas. Esses tipos de vulnerabilidades devem ser incluídos ao considerar a identificação de fontes para a descoberta de vulnerabilidades.

As fontes identificadas de informações sobre vulnerabilidades devem estar alinhadas às necessidades de identificação e análise de vulnerabilidades da <Instituição>.

E05-AMEAÇAS-01-B

As informações sobre vulnerabilidades de cibersegurança são coletadas e interpretadas para a <Instituição>

Detalhamento:

A <Instituição> deve ter um processo para coletar, catalogar e filtrar informações de vulnerabilidades das fontes identificadas para separar as informações relevantes para a <Instituição>.

E05-AMEAÇAS-01-C

Avaliações de vulnerabilidades em cibersegurança são realizadas

Detalhamento:

Existem muitos tipos de técnicas de avaliação que uma empresa pode usar para descobrir vulnerabilidades, como auditorias e avaliações internas de vulnerabilidades, avaliações de entidades externas, testes de penetração, varreduras baseadas em software e revisão dos resultados de auditorias internas e externas. Vulnerabilidades também podem ser descobertas por meio da revisão e captura a partir da lista padrão de fontes de informações sobre vulnerabilidades da <Instituição>.

E05-AMEAÇAS-01-D

Vulnerabilidades de cibersegurança relevantes para a execução da <Instituição> são mitigadas

Detalhamento:

A <Instituição> responde a vulnerabilidades identificadas por fontes de informação confiáveis (por exemplo, agências governamentais, fornecedor de software) e toma medidas para mitigar essas vulnerabilidades caso possam afetar a prestação dos serviços. Os anúncios de vulnerabilidade podem incluir classificações de criticidade (como alta, média, baixa). Esses fatores devem ser considerados no contexto do ambiente geral. Mesmo vulnerabilidades de baixa pontuação podem ser relevantes e ter um impacto potencial significativo quando avaliadas em relação ao seu ambiente de TI ou TO. A resposta pode envolver, por exemplo, implementar controles de mitigação, aplicar patches de cibersegurança ou rastrear níveis de patch e versões do sistema operacional dos dispositivos. Técnicas avançadas de cibersegurança, como caça a ameaças e defesa ativa, podem fornecer informações detalhadas sobre o ambiente de TI que apoiam a determinação da relevância de uma vulnerabilidade para a <Instituição>. É importante notar que a implementação de novos controles compensatórios pode exigir a alocação de recursos adicionais, como pessoas, recursos e ferramentas, além do orçamento atual do programa de cibersegurança.

E05-AMEAÇAS-01-E

Fontes de informações sobre vulnerabilidades em cibersegurança que coletivamente abordam ativos de maior prioridade são monitoradas

Detalhamento:

As fontes de informações sobre vulnerabilidades são avaliadas para determinar até que ponto fornecem informações sobre ativos importantes. Fontes que oferecem mais utilidade e valor devem ser priorizadas para maior monitoramento e revisão. a <Instituição> deve identificar fontes adicionais de informações sobre vulnerabilidades se determinar que as fontes existentes não fornecem informações adequadas para quaisquer ativos-chave.

E05-AMEAÇAS-01-F

Avaliações de vulnerabilidades em cibersegurança são realizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

A <Instituição> utiliza métodos estabelecidos, documentados e estruturados de avaliação de vulnerabilidades para identificar vulnerabilidades conhecidas (ou seja, vulnerabilidades identificadas por entidades externas e publicadas em fontes de informação), bem como outras potenciais fraquezas que podem ser exploradas por um adversário. Essas avaliações podem ser conduzidas por funcionários internos ou por uma entidade terceirizada. Deve-se considerar a perspectiva de um potencial ator de ameaça interna ou externa. Isso pode ajudar a identificar vetores de ameaça potenciais que, de outra forma, passariam despercebidos. a <Instituição> deve decidir os intervalos de tempo apropriados que usará para repetir avaliações, garantindo que possua as informações de vulnerabilidade mais atuais e precisas.

E05-AMEAÇAS-01-G

As vulnerabilidades de cibersegurança identificadas são analisadas, priorizadas e tratadas de acordo

Detalhamento:

Vulnerabilidades podem existir em todos os tipos de ativos de TI, incluindo sistemas operacionais, softwares aplicativos, firmware, dispositivos de rede, dispositivos móveis, dispositivos IoT e ativos residindo na nuvem.

a <Instituição> pode melhorar a eficácia da gestão de vulnerabilidades por meio da análise e priorização. A análise pode ajudar na priorização de várias maneiras, como ajudar a identificar o impacto potencial que uma vulnerabilidade pode ter na postura de segurança de uma <Instituição>. Existem vários fatores importantes para determinar o impacto potencial de uma vulnerabilidade. Os atributos da vulnerabilidade — o que ela pode fazer, como é explorada, os efeitos potenciais e os ativos potencialmente afetados — devem ser cuidadosamente considerados.

Além disso, as características individuais do ambiente de TI, os controles de cibersegurança estabelecidos e a avaliação de impacto determinada externamente, como as pontuações do Sistema Comum de Pontuação de Vulnerabilidades (CVSS) do Banco de Dados Nacional de Vulnerabilidades (NVD) do NIST.

Com base nos resultados da análise, uma <Instituição> pode então priorizar vulnerabilidades identificadas para ações futuras. As atividades realizadas para enfrentar vulnerabilidades podem incluir a implementação de patches de software, sistema ou firmware; desenvolvimento e implementação de

soluções operacionais ou outros controles de mitigação; e desenvolvimento e implementação de novos planos de continuidade ou atualização de planos existentes.

E05-AMEAÇAS-01-H

O impacto operacional na função é avaliado antes da implantação de patches ou outras mitigações

Detalhamento:

Os patches propostos, especialmente aqueles que afetam ativos críticos, devem ser testados quanto ao impacto operacional antes da instalação. Testes de patches podem ajudar a identificar efeitos inesperados no ativo ou em outros ativos integrados. a <Instituição> pode decidir testar patches em um ambiente de teste quando viável ou em um número limitado de sistemas de produção não críticos antes da implementação em toda a empresa.

E05-AMEAÇAS-01-I

Informações sobre vulnerabilidades de cibersegurança descobertas são compartilhadas com stakeholders definidos pela <Instituição>

Detalhamento:

À medida que vulnerabilidades de cibersegurança são descobertas por meio de fontes de informações e avaliações de vulnerabilidades, informações sobre vulnerabilidades que seriam importantes para os stakeholders relevantes devem ser compartilhadas com eles.

E05-AMEAÇAS-01-J

Fontes de informações sobre vulnerabilidades em cibersegurança que atendem coletivamente a todos os ativos de TI dentro da <Instituição> são monitoradas

Detalhamento:

As fontes de informações sobre vulnerabilidades devem ser avaliadas para determinar até que ponto fornecem informações para todos os ativos de TI dentro da <Instituição>. Fontes que abordam ativos de maior prioridade e aquelas consideradas de maior importância podem ser priorizadas para maior monitoramento e revisão.

E05-AMEAÇAS-01-K

Avaliações de vulnerabilidades em cibersegurança são realizadas por partes independentes das operações da <Instituição>

Detalhamento:

Além das avaliações de vulnerabilidade realizadas internamente, a <Instituição> deve periodicamente ter partes externas para realizar avaliações a fim de obter uma perspectiva completamente objetiva. Os avaliadores devem ser externos às operações da <Instituição>, mas não necessariamente externos à <Instituição>.

E05-AMEAÇAS-01-L

As atividades de monitoramento de vulnerabilidades incluem revisão para confirmar que as ações tomadas em resposta a vulnerabilidades de cibersegurança foram eficazes

Detalhamento:

Após uma resposta ser feita para corrigir uma vulnerabilidade (como a implantação de patches), o monitoramento é realizado para garantir que a resposta tenha sido eficaz. Os métodos para confirmar a eficácia variarão dependendo dos recursos disponíveis para o programa de cibersegurança e do tipo de tratamento escolhido para uma vulnerabilidade. Por exemplo, se um fornecedor de sistemas operacionais divulgou a presença de uma vulnerabilidade, a <Instituição> pode optar por corrigir a vulnerabilidade e aplicar um patch. Depois, uma varredura de vulnerabilidade pode ser usada para confirmar que a vulnerabilidade foi resolvida nos sistemas afetados. Técnicas avançadas de cibersegurança, como caça a ameaças e defesa ativa, também podem ser usadas como métodos de verificação.

E05-AMEAÇAS-01-M

Mecanismos são estabelecidos e mantidos para receber e responder a relatórios do público ou de partes externas sobre potenciais vulnerabilidades relacionadas aos ativos de TI da <Instituição>, como sites públicos ou aplicativos móveis

Detalhamento:

Caso um indivíduo externo à <Instituição> identifique uma vulnerabilidade em um ativo de TI ou TO dentro da <Instituição>, seria benéfico que a <Instituição> fosse notificada. O desenvolvimento de um processo que se integre às atividades existentes de gestão de vulnerabilidades possibilitaria melhor o programa de cibersegurança na identificação de vulnerabilidades. Esse mecanismo deve permitir que a <Instituição> receba comunicações e tome as ações necessárias (por exemplo, análise e teste para verificar a existência de uma vulnerabilidade relatada). O mecanismo implementado deve complementar as atividades atuais de gestão de vulnerabilidades e a <Instituição> deve considerar se o mecanismo exigiria recursos adicionais. Por exemplo, se um bug em um site permite que um atacante acesse informações não autorizadas, a pessoa que descobriu a vulnerabilidade envia um e-mail para um endereço especificado com detalhes sobre a vulnerabilidade. Essa funcionalidade pode ser implementada de várias maneiras, como configurar um formulário web, um endereço de e-mail dedicado ou por meio de um serviço de terceiros.

E05-AMEAÇAS-02

Responder a ameaças e compartilhar informações sobre ameaças

E05-AMEAÇAS-02-A

Fontes de informação internas e externas para apoiar as atividades de gerenciamento de ameaças são identificadas

Detalhamento:

A <Instituição> deve pesquisar periodicamente fontes de informação (como CISA, ISACs apropriados, associações industriais, fornecedores e briefings federais) para determinar sua relevância e valor no fornecimento de informações sobre ameaças. Algumas análises podem ser necessárias primeiro para determinar quais informações são mais relevantes para apoiar as atividades de gerenciamento de ameaças.

Além disso, ameaças que afetam setores industriais semelhantes podem ser relevantes para a <Instituição> e devem ser consideradas de acordo.

E05-AMEAÇAS-02-B

Informações sobre ameaças de cibersegurança são coletadas e interpretadas para a <Instituição>

Detalhamento:

A identificação e resposta a ameaças começa com a coleta de informações úteis sobre ameaças de fontes confiáveis e a determinação se e como essas informações são relevantes no contexto da <Instituição> e da <Instituição>. A coleta e revisão das informações sobre ameaças pode ser feita por funcionários internos, prestada como um serviço por meio de um fornecedor, ou uma combinação de ambos. As fontes de informações sobre ameaças devem abordar os diferentes tipos de ativos de TI, TO e informações que são importantes para a execução da <Instituição>.

E05-AMEAÇAS-02-C

Os objetivos de ameaça para a <Instituição> são identificados

Detalhamento:

Objetivos de ameaça são os potenciais resultados das atividades dos agentes de ameaça que são preocupantes porque teriam impactos negativos na <Instituição>. Por exemplo, uma <Instituição> que não processa dados confidenciais pode não se preocupar com roubo de dados, mas pode estar muito preocupada com um incidente que cause uma interrupção operacional. Os agentes de ameaça podem utilizar múltiplas técnicas, técnicas e procedimentos (TTPs) como as definidas nos frameworks MITRE ATT&CK (para Sistemas de Controle Empresarial ou Industrial) para alcançar seus objetivos. Exemplos de objetivos de ameaça podem incluir manipulação de dados, roubo de propriedade intelectual, danos à propriedade, negação de controle, perda de segurança ou interrupção operacional. Os objetivos de ameaça são contextuais para a <Instituição> e para os ativos dentro da <Instituição>. Por exemplo, uma <Instituição> que não processa dados confidenciais pode não se preocupar com roubo de dados, mas pode estar muito preocupada com um incidente que cause uma interrupção operacional.

E05-AMEAÇAS-02-D

Ameaças relevantes para a execução da <Instituição> são abordadas

Detalhamento:

A <Instituição> responde a ameaças identificadas por meio da coleta e análise de informações sobre ameaças quando se determina que têm potencial para afetar negativamente a <Instituição>. Ameaças relevantes são aquelas que têm os meios, motivos e oportunidades para afetar a prestação dos serviços. A resposta a ameaças pode envolver, por exemplo, a implementação de controles mitigadores ou o monitoramento do status da ameaça.

E05-AMEAÇAS-02-E

É estabelecido um perfil de ameaça para a <Instituição>, que inclui objetivos de ameaça e características adicionais de ameaça (por exemplo, tipos de atores ameaçadores, motivos, capacidades e alvos)

Detalhamento:

O perfil de ameaça pode ser construído a partir de informações sobre ameaças provenientes de fontes confiáveis, tanto internas (como resultados de avaliações de ameaças) quanto externas (como E-ISAC, CISA Central e briefings governamentais). O perfil de ameaça pode ser usado para orientar a

identificação e descrição de ameaças específicas e pode ser utilizado como entrada no processo de análise de risco descrito no <Eixo> de Gestão de Riscos e em atividades de consciência situacional descritas no <Eixo> de Consciência Situacional.

Um perfil de ameaça também pode ajudar a orientar a identificação de ativos dentro da <Instituição> que podem ser aproveitados para alcançar um objetivo de ameaça conforme descrito no <Eixo> de Gestão de Ativos, Mudanças e Configuração. O desenvolvimento de um perfil de ameaça pode ocorrer antes da conclusão de uma autoavaliação ou após a conclusão de uma autoavaliação como uma atividade identificada como parte da análise de lacunas e remediação.

E05-AMEAÇAS-02-F

Fontes de informações sobre ameaças que abordam coletivamente todos os componentes do perfil de ameaça são priorizadas e monitoradas

Detalhamento:

As fontes de informações sobre ameaças são avaliadas para determinar até que ponto fornecem informações necessárias no perfil de ameaça. Fontes de maior valor são priorizadas para maior monitoramento e maior fiscalização. Fontes que não contribuem para abordar componentes do perfil de ameaça são eliminadas ou recebem menos atenção.

E05-AMEAÇAS-02-G

As ameaças identificadas são analisadas, priorizadas e tratadas de acordo

Detalhamento:

As ameaças devem ser avaliadas para determinar quais merecem mais e mais rápida atenção, com base em sua provável intenção, capacidade, alvo e potencial de impactar negativamente a <Instituição> conforme descrito no perfil de ameaça.

As ameaças devem ser tratadas em ordem de prioridade para facilitar uma resposta eficaz. As ações tomadas podem ser analisar a ameaça para compreender melhor o impacto potencial, implementar controles para mitigar o risco associado à ameaça ou ajustar as atividades de monitoramento para buscar indicadores da ameaça.

E05-AMEAÇAS-02-H

Informações sobre ameaças são trocadas com partes interessadas (por exemplo, executivos, equipe de operações, governo, <Instituições> conectadas, fornecedores, <Instituições> do setor, reguladores, Centros de Compartilhamento e Análise de Informações [ISACs])

Detalhamento:

Identifique quais tipos de informações sobre ameaças você está disposto e autorizado a compartilhar ou é obrigado a relatar e estabeleça relacionamentos e processos de comunicação para compartilhar essas informações com outras pessoas. As atividades de compartilhamento de informações devem estar em conformidade com seus requisitos legais e regulatórios.

Para que o compartilhamento de informações sobre ameaças seja eficiente e significativo, alguma análise deve ser feita para garantir que todos os stakeholders relevantes tenham sido identificados e estejam sendo devidamente envolvidos nas atividades de gestão de ameaças. Uma técnica de mapeamento de stakeholders pode ajudar a alcançar isso.

E05-AMEAÇAS-02-I

O perfil de ameaça da <Instituição> é atualizado periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

A <Instituição> deve definir um cronograma para revisar e atualizar o perfil de ameaças estabelecido para a <Instituição>, a fim de garantir que a provável intenção, capacidade e alvo das ameaças atualmente definidas ainda estejam precisas e relevantes, além de adicionar quaisquer novas ameaças identificadas. Considerando que novas ameaças surgem diariamente, a <Instituição> deve considerar dedicar recursos à revisão contínua das informações sobre ameaças e à atualização do perfil de ameaça, se possível.

E05-AMEAÇAS-02-J

Atividades de monitoramento e resposta a ameaças aproveitam e acionam estados de operação predefinidos

Detalhamento:

Estados de operação predefinidos são modos operacionais distintos (que normalmente incluem configurações específicas de TI, bem como procedimentos alternativos ou modificados) que foram projetados e implementados para a <Instituição> e podem ser invocados por um processo manual ou automatizado em resposta a um evento, um ambiente de risco em mudança ou outros dados sensoriais e de conscientização para proporcionar maior segurança, resiliência, confiabilidade e/ou cibersegurança.

Por exemplo, um ISAC publica um boletim notificando seus membros sobre uma campanha bem-sucedida direcionada a seus pares que explora uma vulnerabilidade até então desconhecida a uma tecnologia crítica para a execução da entrega da <Instituição>. Com base nessas informações, nos controles existentes e na postura de risco, a <Instituição> considera a ameaça relevante. Ele invoca um processo de decisão que resulta na declaração de um estado operacional de alta segurança, sacrificando eficiência e facilidade de uso em favor de maior segurança, bloqueando acessos remotos e exigindo um nível mais alto de autenticação e autorização para certos comandos. Monitoramento contínuo dos sistemas internos e do ambiente de ameaça é empregado para determinar quando retornar ao estado normal de operação.

E05-AMEAÇAS-02-K

Métodos seguros e quase em tempo real são usados para receber e compartilhar informações de ameaças, permitindo análises e ações rápidas

Detalhamento:

Integrar um sistema de produtos de cibersegurança potencialmente diversos em uma plataforma responsiva e resiliente de detecção, análise, resposta e compartilhamento de informações requer o uso de padrões de automação de cibersegurança. Esses sistemas têm a intenção de aliviar o ônus sobre os analistas, absorvendo e enriquecendo dados e, em alguns casos, agindo automaticamente em resposta a indicadores maliciosos. Garantir que os componentes de um sistema maior de cibersegurança compartilhem uma taxonomia comum (por exemplo, Expressão Estruturada de Informações sobre Ameaças (STIX), Troca Automatizada Confiável de Informações Indicadoras (TAXII)) e sejam

projetados para aceitar, processar e distribuir dados de diversas fontes e fornecedores com segurança é fundamental para desenvolver uma plataforma de cibersegurança bem-sucedida.

E06-RISCOS

Gestão de Riscos

Resumo:

O ciber-risco é definido como a possibilidade de dano ou perda devido ao acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados de ativos de TI, TO ou informações. O ciber-risco é um componente do ambiente de risco geral e alimenta a estratégia e o programa de gerenciamento de riscos corporativos de uma <Instituição>. O ciber-risco não pode ser eliminado, mas pode ser gerenciado por meio de processos de tomada de decisão informados.

Detalhamento:

O <Eixo> de Gestão de Riscos é um <Eixo> focado na <Instituição> como um todo. As <Ações> descritas em <Eixos> focados na <Instituição> são frequentemente realizadas como parte de um programa corporativo e podem ser estabelecidas e operar independentemente da função em questão. Para levar isso em consideração, o objetivo inicial em cada <Eixo> focado na <Instituição> é o estabelecimento e a manutenção do programa relacionado.

Gerenciar o ciber-risco envolve enquadrar, identificar e avaliar, responder (aceitar, evitar, mitigar, transferir) e monitorar os riscos de uma maneira alinhada com as necessidades da <Instituição>. A chave para realizar essas <Ações> é um entendimento comum da estratégia de gerenciamento de ciber-riscos. Uma estratégia de gerenciamento de ciber-risco fornece orientação para analisar e priorizar o ciber-risco e define a tolerância ao risco. A estratégia de gerenciamento do ciber-risco pode incluir uma metodologia de análise de risco, estratégia de monitoramento de risco e uma descrição de como o programa de ciber-risco será governado. A estratégia de gerenciamento de ciber-riscos deve estar alinhada com a estratégia de gerenciamento de riscos corporativos para garantir que o ciber-risco seja gerenciado de maneira consistente com a missão e os objetivos de negócios da <Instituição>.

Os ciber-riscos são identificados, categorizados e priorizados de forma a ajudar a <Instituição> a responder e monitorar os riscos de forma consistente. Um registro de riscos – uma lista de riscos identificados e atributos associados – também facilita esse processo. A consolidação de riscos em categorias permite que a <Instituição> desenvolva um registro de riscos que reflita o ambiente de risco atual e possa ser gerenciado de forma eficaz com os recursos disponíveis. Outros <Eixos> do modelo (Consciência Situacional; Resposta a Eventos e Incidentes, Continuidade de Operações; e Arquitetura de Cibersegurança) referem-se a práticas de risco e ilustram como as práticas do modelo são fortalecidas à medida que se conectam por meio de um programa de gerenciamento de ciber-riscos.

As informações geradas por meio de <Ações> nos <Eixos> Gerenciamento de Ameaças e Vulnerabilidades e Gerenciamento de Riscos de Terceiros são usadas para atualizar os ciber-riscos e identificar novos riscos.

E06-RISCOS-01

Estabelecer e manter a estratégia e o programa de gerenciamento de ciber-riscos

E06-RISCOS-01-A

A <Instituição> possui uma estratégia para gestão de riscos cibernéticos

Detalhamento:

A <Instituição> desenvolve, implementa e mantém uma estratégia de gestão de riscos de cibersegurança que, em sua forma mais simples, inclui uma lista de objetivos de gestão de riscos cibernéticos e ações, atividades e tarefas relacionadas, além de um plano para implementá-las.

Para um programa baseado nessa metodologia, as áreas de atuação da estratégia podem se alinhar com os objetivos do <Eixo> RISCO e suas <Ações> associadas. Por exemplo, a estratégia pode incluir informações importantes sobre os processos da <Instituição> para identificar, analisar e responder a riscos cibernéticos. Mais detalhes podem incluir as categorias de alto nível em que os riscos são consolidados, critérios para determinar prioridade de risco cibernético e um resumo das técnicas de resposta ao risco a serem aplicadas aos riscos, além da atribuição de responsabilidade pela implementação da estratégia.

E06-RISCOS-01-B

Uma estratégia para gestão de riscos cibernéticos é estabelecida e mantida em alinhamento com a estratégia do programa de cibersegurança (PROGRAMA-1b) e a arquitetura empresarial da <Instituição>

Detalhamento:

A estratégia de gestão de riscos é mantida atualizada e relevante. Uma estratégia de gestão de riscos focada em mitigar riscos de software adquirido, por exemplo, provavelmente estará fora de sintonia com o objetivo de um programa de cibersegurança de aumentar o software desenvolvido internamente e com a meta de arquitetura empresarial que implementa um processo de desenvolvimento seguro.

E06-RISCOS-01-C

O programa de gestão de riscos cibernéticos é estabelecido e mantido para realizar atividades de gestão de riscos cibernéticos de acordo com a estratégia de gestão de riscos cibernéticos

Detalhamento:

O programa de gestão de riscos cibernéticos é tipicamente responsável por garantir que os objetivos de gestão de riscos cibernéticos, conforme documentados na estratégia do programa de gestão de riscos cibernéticos, sejam alcançados. Por exemplo, o programa de gestão de riscos cibernéticos inclui atividades para garantir que a <Instituição> identifique, analise e responda a riscos cibernéticos.

E06-RISCOS-01-D

Informações das atividades do <Eixo> RISCO são comunicadas aos stakeholders relevantes

Detalhamento:

O programa de gestão de riscos possui procedimentos que definem critérios como os tipos de informações que devem ser comunicadas às partes interessadas, métodos de comunicação e gatilhos que exigiriam escalonamento. À medida que a <Instituição> identifica, analisa e responde aos riscos, os stakeholders devem receber informações atualizadas sobre o status dos riscos. Esses stakeholders podem ser internos ou externos à <Instituição>.

E06-RISCOS-01-E

A governança para o programa de gestão de riscos cibernéticos é estabelecida e mantida

Detalhamento:

A <Instituição> pode estabelecer uma posição de oficial de risco de nível superior que supervisione a gestão de riscos ou atribuir a responsabilidade a alguém com autoridade suficiente na <Instituição>. O oficial seria responsável por patrocinar e supervisionar as políticas e procedimentos para as atividades

de gestão de riscos cibernéticos. Outras responsabilidades podem incluir garantir que ciclos de feedback estejam em vigor para avaliar o desempenho das atividades ou fornecer relatórios aos gestores de alto nível sobre o cumprimento das obrigações de conformidade.

E06-RISCOS-01-F

O patrocínio da alta administração para o programa de gestão de riscos cibernéticos é visível e ativo

Detalhamento:

O patrocínio visível e ativo da alta administração pode incluir comunicações regulares da alta administração sobre a importância e o valor do programa de risco cibernético, apoio organizacional para estabelecer e implementar governança para gestão do risco cibernético, e financiamento de prêmios e programas de reconhecimento para funcionários que contribuem significativamente para alcançar os objetivos de cibersegurança.

E06-RISCOS-01-G

O programa de gestão de riscos cibernéticos está alinhado com a missão e os objetivos da <Instituição>

Detalhamento:

O programa de gestão de riscos cibernéticos pode ser um componente de um programa de Gestão de Riscos Empresariais (ERM) ou pode ser um programa independente. Se fizer parte de um ERM, o programa de risco cibernético deve ser modelado segundo o programa empresarial para garantir que as partes interessadas estejam engajadas de forma eficiente e que as informações de risco cibernético possam ser mais facilmente integradas às atividades gerais de ERM.

Um programa independente deve utilizar a estratégia de gestão de riscos cibernéticos, juntamente com a missão e os objetivos da <Instituição>, para construir a direção das atividades do programa por meio de documentos como políticas e procedimentos. Os stakeholders relevantes devem ser engajados para garantir que as atividades do programa estejam alinhadas com as áreas operacionais e de negócios da <Instituição>.

Independentemente de o programa ser independente ou parte de um ERM, o programa de risco cibernético deve levar em conta o apetite pelo risco da <Instituição> ao formar atividades em nível de programa. O apetite pelo risco da <Instituição> é a quantidade de risco que ela está disposta a aceitar, conforme definido pela alta liderança. Certos limiares ou limites podem ser estabelecidos que indicariam se o risco é maior que os níveis de aceitação organizacional.

E06-RISCOS-01-H

O programa de gestão de riscos cibernéticos é coordenado com o programa de gestão de riscos em toda <Instituição>

Detalhamento:

O alinhamento dessas estratégias evita expectativas desalinhadas entre partes interessadas do negócio e técnicas. Por exemplo, os objetivos empresariais de proteger propriedade intelectual e dados empresariais sensíveis são apoiados pelos objetivos de cibersegurança de minimizar superfícies de ataque e estabelecer padrões seguros. Os riscos cibernéticos devem ser comunicados como componentes ou contribuintes para o risco geral e devem ser comunicados nos mesmos termos sempre que possível.

Dentro de uma empresa que não possui funções de gestão de riscos empresariais, esta <Ação> pode ser implementada alinhando as <Ações> de gestão de riscos às funções de gestão em nível empresarial e garantindo que as atividades de <Eixo> estejam ocorrendo no nível empresarial, conforme apropriado (por exemplo, estabelecimento de estratégia, governança de programas de gestão de riscos, comunicação com partes interessadas e liderança, recursos, atribuição de funções e responsabilidades, monitoramento da eficácia).

E06-RISCOS-02

Identificar o ciber-risco

E06-RISCOS-02-A

Os riscos cibernéticos são identificados

Detalhamento:

A identificação de riscos cibernéticos é uma atividade fundamental de gestão de riscos. Ela exige que a <Instituição> identifique os tipos de ameaças, vulnerabilidades e eventos disruptivos que podem representar risco à capacidade operacional dos ativos e serviços. Os riscos identificados formam uma linha de base a partir da qual um processo contínuo de gestão de riscos pode ser estabelecido e gerenciado.

E06-RISCOS-02-B

Um método definido é usado para identificar riscos cibernéticos

Detalhamento:

Um método definido é planejado antecipadamente, claramente descrito, tornado definido e padronizado. Empregar um método definido para identificar riscos ajudará o programa de gestão de riscos cibernéticos a produzir resultados consistentes e a possibilitar uma gestão eficaz do risco cibernético. a <Instituição> pode optar por definir seu próprio método ou utilizar orientações padronizadas, como o NIST SP 800-30, Guia para Condução de Avaliações de Risco.

E06-RISCOS-02-C

Partes interessadas das áreas de operações e negócios apropriadas participam da identificação de riscos cibernéticos

Detalhamento:

O envolvimento de partes interessadas de várias partes da <Instituição> é benéfico, pois diferentes perspectivas de toda a <Instituição> levarão a uma identificação mais abrangente dos riscos. Stakeholders das áreas operacionais podem ter uma melhor compreensão de como um risco pode impactar um processo operacional, enquanto os stakeholders em uma área de negócios podem ter mais visibilidade sobre o impacto de um risco entre os serviços.

E06-RISCOS-02-D

Os riscos cibernéticos identificados são consolidados em categorias (por exemplo, vazamentos de dados, erros internos, ransomware, tomada de controle por TO) para facilitar a gestão no nível da categoria

Detalhamento:

Categorias de risco cibernético são estabelecidas e podem ser baseadas em riscos operacionais comuns, como vazamentos de dados, erros internos, ransomware ou tomada de controle por TO. a <Instituição> deve determinar a granularidade necessária para gerenciar eficazmente os riscos cibernéticos. Após a identificação de um risco cibernético, ele deve ser atribuído a uma das categorias definidas. As categorias ajudarão a <Instituição> a analisar e responder de forma mais eficaz aos riscos. As categorias de risco cibernético podem fazer parte de uma taxonomia maior mantida pelo programa de gestão de riscos da <Instituição>, que inclui termos-chave e definições. Essa capacidade ajudará a permitir que A <Instituição> gerenciem riscos em nível de categoria, mas gerenciar riscos em nível de categoria não é necessário para a implementação desta <Ação>.

E06-RISCOS-02-E

Categorias de risco cibernético e riscos cibernéticos são documentadas em um registro de riscos ou outro artefato

Detalhamento:

O registro de riscos é um inventário de todos os riscos identificados e seus atributos, como suas declarações de risco, prioridades, categoria de risco (conforme definida no RISCO-2d) e dados de avaliação de impacto. O registro de riscos garante que todos os riscos identificados sejam gerenciados e que todos os funcionários envolvidos nas atividades de gestão de riscos estejam utilizando as mesmas informações de risco. O registro de risco pode ser usado para gerenciar riscos individualmente ou em nível de categoria, conforme definido no RISCO-2d. Por exemplo, se um analista identificar novos indicadores que alteram um risco previamente identificado, eles podem ser adicionados ao registro e assim a informação fica disponível para todos os stakeholders da gestão de riscos.

E06-RISCOS-02-F

Categorias de risco cibernético e riscos cibernéticos são atribuídos aos detentores de riscos

Detalhamento:

O proprietário do risco deve ser a pessoa que tem autoridade e autorização dentro da <Instituição> para tomar decisões sobre como responder a categorias e riscos específicos e para atribuir orçamento para as respostas ao risco. Lembre-se de que uma resposta legítima (mas potencialmente prejudicial) a um risco é aceitá-lo. O proprietário do risco deve ter autoridade para aceitar um risco.

Para que um proprietário de risco aceite plenamente um risco, é importante que ele compreenda o risco e os impactos potenciais que podem ocorrer caso o risco seja realizado. Para determinar se um proprietário do risco tem autoridade adequada para aceitar um risco, pode ajudar considerar se os impactos potenciais do risco podem ir além do escopo de sua autoridade. Também pode ajudar considerar se o potencial proprietário do risco possui autoridade e recursos adequados sob sua responsabilidade para fazer mudanças apropriadas caso o risco seja considerado fora da tolerância ao risco da <Instituição>.

A atribuição de um risco a um proprietário do risco pode envolver algum tipo de atestação escrita de sua posse do risco. A atribuição de propriedade no nível certo de autoridade ajuda a garantir que as respostas ao risco sejam executadas de forma eficaz.

E06-RISCOS-02-G

Atividades de identificação de risco cibernético são realizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

Riscos cibernéticos que podem afetar ativos de TI, TO e informação devem ser identificados e abordados para gerenciar ativamente a resiliência desses ativos e, mais importante, os serviços aos quais esses ativos estão conectados. a <Instituição> pode usar um método estruturado de avaliação de riscos para identificar esses riscos de acordo com gatilhos, como mudanças no sistema e eventos externos, conforme estabelecido na estratégia de gestão de riscos.

As avaliações de risco fornecem as informações necessárias para determinar se os riscos identificados estão dentro das tolerâncias de risco da <Instituição>. As avaliações também levam em conta as mitigações e proteções existentes como parte do processo. Riscos identificados por meio de avaliações devem ser adicionados ao registro de riscos, conforme recomendado no RISCO-2e.

E06-RISCOS-02-H

As atividades de identificação de risco cibernético aproveitam informações de inventário e priorização de ativos do <Eixo> ATIVO, como suporte final de ativos de TI, pontos únicos de falha, risco de divulgação, adulteração ou destruição de ativos de informação

Detalhamento:

A interrupção da produtividade dos ativos devido ao risco operacional afeta a capacidade das funções associadas de cumprir sua missão. Assim, o escopo das avaliações de risco deve focar em ativos e atividades cuja interrupção tem maior impacto potencial na garantia da missão. O inventário de ativos deve incluir critérios que identifiquem os ativos mais críticos para a <Instituição>.

E06-RISCOS-02-I

As informações de gerenciamento de vulnerabilidades das atividades do <Eixo> AMEAÇA são usadas para atualizar riscos cibernéticos e identificar novos riscos (como riscos decorrentes de vulnerabilidades que representam um risco contínuo para a <Instituição> ou vulnerabilidades recém-identificadas)

Detalhamento:

Fontes de informações sobre vulnerabilidades identificadas no <Eixo> AMEAÇA devem ser usadas em conjunto com o processo de gestão de riscos para identificar novos riscos e atualizar riscos existentes. Por exemplo, um novo risco deve ser identificado se um fornecedor divulgar publicamente uma vulnerabilidade que afete um ativo de TI.

E06-RISCOS-02-J

As informações de gerenciamento de ameaças das atividades do <Eixo> AMEAÇA são usadas para atualizar riscos cibernéticos e identificar novos riscos

Detalhamento:

Fontes de informação sobre ameaças identificadas no <Eixo> AMEAÇA devem ser usadas em conjunto com o processo de gestão de riscos para identificar novos riscos e atualizar riscos existentes. Por exemplo, um novo risco deve ser identificado se a inteligência de ameaças indicar que um ator de ameaça pode estar mirando a <Instituição>.

E06-RISCOS-02-K

Informações das atividades do <Eixo> de TERCEIROS são usadas para atualizar riscos cibernéticos e identificar novos riscos

Detalhamento:

Informações das atividades de TERCEIROS devem ser usadas para identificar novos riscos e atualizar riscos existentes. Por exemplo, se informações de fonte aberta indicarem que um fornecedor de equipamentos foi violado, a <Instituição> deve considerar o impacto e registrar um risco no registro de riscos.

E06-RISCOS-02-L

Informações das atividades do <Eixo> ARQUITETURA (como lacunas de conformidade arquitetônica sem mitigação) são usadas para atualizar riscos cibernéticos e identificar novos riscos

Detalhamento:

Avaliações periódicas ou contínuas devem ser utilizadas para determinar lacunas de conformidade entre os sistemas e redes da <Instituição> e a arquitetura de cibersegurança. Lacunas na conformidade devem ser registradas à medida que os riscos e planos de remediação forem formados para fechar essas lacunas. Os planos de remediação devem incluir informações como recursos necessários para concluir a remediação e datas até os quais a remediação será concluída.

E06-RISCOS-02-M

A identificação de riscos cibernéticos considera riscos que podem surgir ou impactar infraestrutura crítica ou outrA <Instituição> interdependentes

Detalhamento:

Interdependências que existam com outros SEICs devem ser compreendidas. Se um serviço de utilidade ou outro serviço dependente não estiver disponível por um período significativo, a <Instituição> deve entender como isso impactaria as operações. Por exemplo, se um desastre natural está impactando a capacidade de um provedor de serviços de internet de fornecer serviços de internet, riscos que decorram de comunicações degradadas entre unidades organizacionais geograficamente dispersas e como isso impactem a <Instituição> devem ser considerados e registrados no registro de riscos.

E06-RISCOS-03

Analisar o ciber-risco

E06-RISCOS-03-A

Os riscos cibernéticos são priorizados com base no impacto estimado

Detalhamento:

O impacto potencial dos riscos identificados para a <Instituição> deve ser avaliado e utilizado para priorizar os riscos cibernéticos. Um risco cibernético de prioridade maior deve receber maior atenção ao determinar possíveis mitigações ou respostas. A priorização deve focar em critérios considerados importantes para a empresa, como impactos de segurança, impactos operacionais e financeiros (por exemplo, custo de recuperação, custo potencial de inatividade ou perda de dados). A priorização pode usar métodos qualitativos para indicar o nível relativo de impacto (por exemplo, Alto, Médio, Baixo).

E06-RISCOS-03-B

Critérios definidos são usados para priorizar riscos cibernéticos (por exemplo, impacto na <Instituição>, impacto na comunidade, probabilidade, suscetibilidade, tolerância ao risco)

Detalhamento:

As possíveis consequências e outros aspectos dos riscos identificados devem ser avaliados e priorizados usando os critérios de risco de forma consistente. Os riscos podem ser categorizados por origem, tipo de ameaça ou outra característica em comum. Essa análise ajuda a determinar quais riscos merecem mais atenção, considerando as circunstâncias operacionais únicas da <Instituição>, bem como a rapidez com que devem ser tratados.

Uma prioridade relativa deve ser atribuída a cada risco (talvez por categoria) usando um esquema de priorização consistente. A intenção da priorização é determinar os riscos cibernéticos que mais precisam de atenção devido ao seu potencial de afetar as operações. Componentes típicos de uma abordagem para priorização de riscos incluem diagramas de fluxo que representam o processo de priorização, entradas e saídas do processo, uma lista de partes interessadas relevantes envolvidas na priorização de riscos e um esquema para classificar riscos (alto, médio, baixo etc.).

A categorização e priorização dos riscos ajudam a ajustar o tamanho correto do número de riscos gerenciados, assim como do tempo e esforço que uma <Instituição> dedica à gestão dos riscos cibernéticos identificados.

E06-RISCOS-03-C

Um método definido é usado para estimar o impacto de riscos cibernéticos de prioridade mais alta (por exemplo, comparação com eventos reais, quantificação de risco)

Detalhamento:

Um método definido para estimar o impacto de riscos e categorias de risco (por exemplo, impactos de segurança, interrupções operacionais, custo potencial de tempo de inatividade, custo de dados perdidos e custo de recuperação) é benéfico, pois fornece um ponto comum de comparação para riscos. Esse método ajuda a identificar e priorizar os riscos mais críticos que podem impactar as operações. Métodos matemáticos ou estatísticos podem ser usados para determinar um valor, como o custo potencial caso um risco seja realizado.

E06-RISCOS-03-D

Métodos definidos são usados para analisar riscos cibernéticos de prioridade mais alta (por exemplo, analisar a prevalência de tipos de ataques para estimar a probabilidade, usando os resultados das avaliações de controles para estimar a suscetibilidade)

Detalhamento:

Um método definido para analisar riscos e categorias de risco após a priorização garante que as atividades de análise sejam repetíveis e produzam resultados consistentes. Resultados de processos organizacionais ou testes contínuos, como avaliações de controle, podem ajudar a <Instituição> a determinar a suscetibilidade a uma vulnerabilidade recém-identificada.

E06-RISCOS-03-E

Stakeholders organizacionais das operações e funções de negócios apropriadas participam da análise de riscos cibernéticos de maior prioridade

Detalhamento:

Stakeholders organizacionais das áreas apropriadas da <Instituição> são necessários para uma análise abrangente das categorias priorizadas de risco cibernético e riscos cibernéticos. Stakeholders específicos podem ser mais adequados para analisar certos riscos cibernéticos ou categorias de risco cibernético e fornecer insights que não podem ser obtidos de outros membros da <Instituição>.

Além disso, stakeholders de várias partes da <Instituição> fornecerão diferentes perspectivas que ajudarão a obter uma compreensão completa dos riscos e possíveis mitigações.

E06-RISCOS-03-F

Riscos cibernéticos são removidos do registro de riscos ou de outro artefato usado para documentar e gerenciar riscos identificados quando não precisam mais de rastreamento ou resposta

Detalhamento:

Uma vez que a análise feita pelos stakeholders da gestão de riscos indique que a percepção de um risco cibernético não é mais provável ou que o impacto não é material, o risco deve ser removido do registro de riscos ou de outro artefato usado para documentar e gerenciar riscos identificados. Deve ser seguido um processo definido para remover riscos, que inclua o arquivamento de informações de análise e quaisquer lições aprendidas que possam ser aproveitadas na gestão de riscos cibernéticos semelhantes no futuro.

Categorias de risco cibernético que não têm mais função no processo de gestão de riscos também devem ser removidas. À medida que a <Instituição> resolve as causas dos riscos, algumas categorias de risco cibernético podem se tornar desnecessárias ou redundantes.

Remover categorias de risco cibernético e riscos cibernéticos uma vez eliminados ou o impacto não é relevante ajudará a <Instituição> a gerenciar os riscos remanescentes de forma mais eficiente. Por exemplo, a <Instituição> pode remover um risco cibernético relacionado a um sistema operacional se esse sistema operacional não estiver mais em uso dentro da <Instituição>.

E06-RISCOS-03-G

Análises de risco cibernético são atualizadas periodicamente e de acordo com gatilhos definidos, como mudanças no sistema, eventos externos e informações de outros <Eixos> do modelo

Detalhamento:

Riscos cibernéticos que podem afetar TI, TO e ativos de informação devem ser analisados periodicamente ou de acordo com gatilhos definidos para determinar se critérios como impacto ou probabilidade mudaram. Uma maior probabilidade de um risco ser realizado pode levar a uma mudança na prioridade do risco cibernético e a uma estratégia diferente para mitigar o risco cibernético.

Para cada risco cibernético, a <Instituição> deve designar uma data para que o risco deve ser reavaliado ou um gatilho definido que impulsione a reavaliação. Os gatilhos podem incluir uma data em que um ativo não é mais suportado por um fornecedor ou uma métrica interna que excedeu um nível de tolerância.

E06-RISCOS-04

Responder ao ciber-risco

E06-RISCOS-04-A

Respostas ao risco (como mitigar, aceitar, evitar ou transferir) são implementadas para lidar com riscos cibernéticos

Detalhamento:

Uma vez identificados os riscos para a <Instituição>, a <Instituição> deve decidir como responder a esses riscos. A resposta começa com a atribuição de uma disposição de risco a cada risco ou categoria de risco, ou seja, uma declaração da intenção da <Instituição> de enfrentar o risco. Por exemplo, mitigação de riscos envolve tomar medidas ativas para minimizar o risco; A transferência de risco é a transferência contratual de um risco de uma parte para outra por meio de um contrato, como por meio de uma apólice de seguro, uma renúncia de responsabilidade com um cliente ou um acordo de indenização com um fornecedor.

Respostas ao risco devem ser desenvolvidas como parte da estratégia de gestão de riscos. As respostas ao risco podem variar bastante entre organizações, mas normalmente incluem:

• Evitar riscos — alterar operações para evitar o risco enquanto ainda fornece o serviço essencial

• Aceitação do risco — reconhecimento do risco, mas conscientemente não tomar nenhuma ação (em essência, aceitar as possíveis consequências do risco)

• Transferência de riscos — atribuir o risco a uma entidade disposta e capaz

• Mitigação de riscos — adotar medidas ativas para minimizar o risco

• Monitoramento de risco—realizar pesquisas adicionais e adiar a ação sobre o risco até que a necessidade de abordá-lo seja evidente

Os processos organizacionais de seleção de resposta ao risco devem esclarecer que não é necessário mitigar todos os riscos identificados. A evitação, aceitação ou transferência de riscos deve ser considerada além da mitigação.

E06-RISCOS-04-B

Um método definido é usado para selecionar e implementar respostas ao risco com base na análise e priorização

Detalhamento:

A <Instituição> deve desenvolver uma lista definida de respostas ao risco aceitáveis e a definição de cada resposta. Pode ser necessário definir aprovações que são necessárias para certas estratégias de resposta ao risco, como aceitar um risco. Processos para outras estratégias de resposta a riscos, como transferência, também devem ser considerados para garantir que os riscos cibernéticos tenham um indivíduo responsável por rastreá-los até o fechamento.

E06-RISCOS-04-C

Os controles de cibersegurança são avaliados para determinar se são projetados adequadamente e operam conforme o objetivo para mitigar os riscos cibernéticos identificados

Detalhamento:

A eficácia do controle de cibersegurança deve ser avaliada comparando o resultado pretendido dos controles de cibersegurança com o resultado real. a <Instituição> pode usar métricas de desempenho ou outros indicadores definidos para identificar controles de cibersegurança que não foram projetados adequadamente. Por exemplo, se um dispositivo de autenticação biométrica tiver alta taxa de falsos negativos e exceções forem feitas para acesso de pessoal, a configuração do controle deve ser avaliada para determinar se a sintonia é necessária para melhorar o desempenho do dispositivo.

E06-RISCOS-04-D

Os resultados das análises de impacto de risco cibernético e das avaliações de controle de cibersegurança são revisados em conjunto pela liderança da empresa para determinar se os riscos cibernéticos são suficientemente mitigados e se as tolerâncias ao risco não são ultrapassadas

Detalhamento:

Insights únicos podem ser obtidos da fusão dos resultados das análises de impacto de risco cibernético e avaliações de controle de cibersegurança. Por exemplo, a liderança empresarial pode determinar que mover alguns sistemas para a nuvem aumenta a disponibilidade e melhora as operações de uma <Instituição>, mas uma avaliação de controle de cibersegurança constata que configurações incorretas do ambiente podem levar ao comprometimento da confidencialidade.

E06-RISCOS-04-E

Respostas ao risco (como mitigar, aceitar, evitar ou transferir) são revisadas periodicamente pela liderança para determinar se ainda são adequadas

Detalhamento:

Respostas ao risco e métodos definidos para implementar respostas ao risco devem ser revisados periodicamente para determinar se ainda são apropriados e eficazes na gestão do risco cibernético para a <Instituição>. Mudanças no ambiente operacional, como novas tecnologias, novos serviços ou novas parcerias estratégicas, podem fazer com que a <Instituição> modifique estratégias de resposta existentes ou crie novas estratégias de resposta.

E07-RESPOSTA

Resposta a Eventos e Incidentes

Resumo:

Um evento de cibersegurança em um sistema ou rede é qualquer ocorrência observável relacionada a um requisito de cibersegurança (confidencialidade, integridade, autenticidade ou disponibilidade de ativos). Um incidente de cibersegurança é um evento ou série de eventos que afeta significativamente ou pode afetar significativamente a infraestrutura crítica ou os ativos e serviços institucionais e exige que a <Instituição> (e possivelmente outras partes interessadas) responda de alguma forma para prevenir ou limitar os impactos adversos.

Detalhamento:

A detecção de eventos de cibersegurança inclui a designação de um fórum para relatar eventos e estabelecer critérios para priorização de eventos. Esses critérios devem estar alinhados com a estratégia de gerenciamento de ciber-riscos discutida no <Eixo> Gerenciamento de Riscos, garantir uma avaliação consistente dos eventos e fornecer um meio de determinar o que constitui um evento de cibersegurança, quando os eventos de cibersegurança devem ser escalados e as condições que justificam a declaração de ciberincidentes. A identificação de eventos e ciberincidentes pode incorporar dados de várias fontes, incluindo os resultados de <Ações> realizadas noutros <Eixos>, como os resultados de <Ações> do <Eixo> Consciência Situacional. Os eventos de cibersegurança podem se originar ou afetar terceiros que necessitam de coordenação no planejamento, execução e comunicações de resposta.

O escalonamento de eventos de cibersegurança envolve a aplicação dos critérios discutidos no <objetivo> Detectar eventos de cibersegurança para determinar quando um evento deve ser escalonado e quando um incidente deve ser declarado. Tanto os eventos de cibersegurança quanto os ciberincidentes devem ser gerenciados de acordo com um plano de resposta. Eventos de cibersegurança e incidentes declarados podem desencadear obrigações externas, incluindo relatórios a órgãos reguladores ou notificação de clientes. Correlacionar vários eventos e ciberincidentes e outros registros pode revelar problemas sistêmicos no ambiente.

A resposta a ciberincidentes exige que a <Instituição> tenha um processo para limitar o impacto dos ciberincidentes em suas unidades funcionais e institucionais. O processo deve descrever como a <Instituição> gerencia todas as fases do ciclo de vida do incidente (por exemplo: triagem, tratamento, comunicação, coordenação e encerramento). Os planos de resposta a incidentes devem ser abrangentes sobre os tipos de incidentes que podem afetar a <Instituição> (por exemplo, ransomware, negação de serviço, interrupção operacional). Os planos de resposta a incidentes também devem abordar possíveis incidentes que possam afetar significativamente a <Instituição>, como grandes divulgações de vulnerabilidades e tecnologias emergentes que reduziriam a eficácia dos controles atuais de cibersegurança (por exemplo, computação quântica). A realização de revisões de lições aprendidas como parte da resposta a eventos e ciberincidentes ajuda a <Instituição> a lidar com os possíveis problemas (por exemplo, vulnerabilidades, lacunas de controle e deficiências de processo) que levaram ao incidente e priorizar futuros esforços de melhoria de longo prazo.

E07-RESPOSTA-01

Detectar eventos de cibersegurança

E07-RESPOSTA-01-A

Eventos de cibersegurança detectados são reportados a uma pessoa ou função especificada e documentados

Detalhamento:

Estabeleça um ponto de coleta para reportar eventos cibernéticos reais ou suspeitos, como um help desk. As informações de contato dessa pessoa, função ou grupo devem ser divulgadas a todos os stakeholders da <Instituição>. O contato deve ser alguém que tenha conhecimento de <Ações> e questões de cibersegurança e que possa documentar com precisão informações de eventos reportados e, possivelmente, até mesmo fazer soluções básicas de problemas. Alternativamente, ou adicionalmente, eventos podem ser reportados por meio de um sistema interno, como um help desk virtual em uma intranet.

E07-RESPOSTA-01-B

Critérios são estabelecidos para a detecção de eventos de cibersegurança (por exemplo, o que constitui um evento de cibersegurança, onde procurar eventos de cibersegurança)

Detalhamento:

A <Instituição> deve definir critérios de detecção de eventos de cibersegurança que especifiquem o que distingue eventos de cibersegurança da multiplicidade de outros eventos. Esses critérios devem estar relacionados aos requisitos de cibersegurança dos ativos de TI, TO e informações importantes para a execução da <Instituição>. Eles permitem que a <Instituição> concentre recursos valiosos (pessoas, ferramentas etc.) em eventos que podem afetar a produtividade desses ativos. Sobre "onde procurar eventos de cibersegurança", certifique-se de considerar eventos potenciais originados por terceiros, como provedores de recursos em nuvem.

E07-RESPOSTA-01-C

Eventos de cibersegurança são documentados com base nos critérios estabelecidos

Detalhamento:

Qualquer evento que seja um evento de acordo com os critérios definidos na RESPOSTA-1b deve ser documentado de maneira consistente. a <Instituição> deve decidir quais detalhes sobre eventos devem ser documentados para possibilitar, por exemplo:

• Decisões sobre declarar eventos como incidentes

• Coleta de dados para quaisquer métricas de evento que a <Instituição> possa estar monitorando

• Correlação das informações do evento, caso a <Instituição> esteja fazendo isso.

E07-RESPOSTA-01-D

As informações de eventos são correlacionadas para a análise de incidentes de suporte identificando padrões, tendências e outras características comuns

Detalhamento:

A correlação de eventos pode ajudar a identificar questões que podem ser mais sérias do que quando os eventos são considerados de forma independente. Por exemplo, ataques de força bruta podem ser ofuscados ao conduzi-los a partir de múltiplas máquinas, contornando assim as regras tradicionais de bloqueio para 3 ou 5 logins falhados de um único endereço IP. E a questão só é reconhecida como

mais séria quando vista em um contexto mais amplo. A correlação de eventos requer a comparação de dois ou mais eventos e estabelece potenciais relações entre eles.

Estes são exemplos de atividades de correlação:

• Visualizando e comparando eventos separados da mesma fonte de informação

• Visualizando e comparando eventos separados de diferentes fontes de informação

• Observando e comparando eventos ao longo do tempo para características comuns

E07-RESPOSTA-01-E

As atividades de detecção de eventos de cibersegurança são ajustadas com base nos riscos identificados e no perfil de ameaça da <Instituição> (AMEAÇA-2e)

Detalhamento:

A detecção de eventos depende em grande parte do grau em que há ampla consciência sobre a gama potencial de eventos que podem afetar a <Instituição>. Uma fonte útil para ampliar a conscientização sobre eventos da <Instituição> são os riscos que foram identificados e estão sendo tratados no processo de gestão de riscos organizacionais. (Veja RISCO-2a.)

Alertas devem ser desenvolvidos para funcionar como indicadores de alerta precoce para cada risco ou ameaça. Para ajustar as atividades de detecção de eventos com base no perfil de ameaça da <Instituição>, a <Instituição> deve revisar os ativos-alvo, objetivos e métodos de ataque que podem ser empregados pelos atores ameaçadores e ajustar os alertas de acordo. Por exemplo, se o relatório de ameaças indicar que adversários estão mirando certos sistemas SCADA, alertas existentes podem ser modificados para disparar em anomalias que correspondam a aspectos desta <Ação> adversarial.

E07-RESPOSTA-01-F

A consciência situacional da <Instituição> é monitorada para apoiar a identificação de eventos de cibersegurança

Detalhamento:

As informações coletadas por meio de atividades de conscientização situacional são revisadas e usadas para ajudar a identificar eventos de cibersegurança. Essas informações podem ser coletadas de múltiplas fontes, incluindo funções dentro e fora da <Instituição>.

E07-RESPOSTA-02

Analisar eventos de cibersegurança e declarar incidentes

E07-RESPOSTA-02-A

Critérios para declarar incidentes de cibersegurança são estabelecidos

Detalhamento:

Critérios para declarar incidentes de cibersegurança são usados para determinar se um evento deve ser tratado como um incidente e qual a gravidade potencial do evento. Uma escala de ranking, como alta, média e baixa, pode ajudar a comunicar a gravidade do incidente aos stakeholders e a priorizar as ações de resposta a serem tomadas.

Os critérios de declaração de incidentes devem ser desenvolvidos a partir da experiência e podem ser parcialmente derivados de critérios de avaliação de risco (como limiares de impacto) estabelecidos como parte das atividades do <Eixo> de Gestão de Riscos. Os critérios podem ser baseados no tipo de

evento (como acesso não autorizado), nível de impacto (por exemplo, local versus <Instituição> em toda a região), tipo de impacto (sistemas internos versus serviços externos críticos), obrigações de conformidade (apenas internamente versus evento reportável) ou tempo médio até a recuperação. Para alguns eventos, o tempo entre a detecção e a declaração de incidente pode ser imediato, exigindo pouca análise adicional. Em outros casos, a <Instituição> pode querer aproveitar critérios previamente desenvolvidos para ajudar a orientar a declaração de incidentes.

E07-RESPOSTA-02-B

Eventos de cibersegurança são analisados para apoiar a declaração de incidentes de cibersegurança

Detalhamento:

A análise de eventos de cibersegurança ajuda a <Instituição> a reunir informações adicionais para resolução de eventos e para auxiliar na declaração, manejo e resposta de incidentes. Essa análise pode consistir em categorizar, correlacionar e priorizar eventos. Por meio da análise, a <Instituição> determina o tipo e a extensão de um evento (por exemplo, físico versus técnico), se o evento se correlaciona com outros eventos (para determinar se são sintomáticos de uma questão, problema ou incidente maior) e em que ordem os eventos devem ser abordados ou atribuídos para declaração, manejo e resposta ao incidente. A análise ajuda a <Instituição> a determinar se o evento precisa ser escalado para outros funcionários organizacionais ou externos (fora da equipe de gerenciamento de incidentes) para análise e resolução adicionais.

E07-RESPOSTA-02-C

Os critérios de declaração de incidentes de cibersegurança são formalmente estabelecidos com base no impacto potencial na função

Detalhamento:

Cada <Instituição> possui muitos fatores únicos que devem ser considerados ao determinar quando um evento deve ser declarado incidente. Por meio da experiência, uma <Instituição> pode ter um conjunto base de tipos de eventos que definem incidentes padrão, como surto de vírus, acesso não autorizado a uma conta de usuário ou ataque de negação de serviço. No entanto, na realidade, a declaração de incidente pode ocorrer de acordo com o evento.

Para orientar a <Instituição> na determinação de quando declarar um incidente (especialmente se a declaração de incidente não for imediatamente aparente), a <Instituição> deve definir critérios de declaração de incidente. Os critérios de declaração de incidente devem incluir fatores que indiquem o impacto potencial na função, tais como:

• Impactos potenciais de segurança

• Impacto funcional (prioridade e escopo dos ativos impactados)

• Impacto informacional (impacto nos ativos informacionais)

• Recuperação do incidente (recursos necessários para a recuperação do incidente)

• A causa potencial do incidente (atividade maliciosa vs. ações não intencionais)

Além disso, os critérios de declaração de incidentes devem considerar o impacto nos objetivos de cibersegurança da <Instituição>, tais como:

• Potencial perda financeira

• Número de clientes afetados

• Interrupção de um sistema de TI importante

• Roubo de informações do cliente

E07-RESPOSTA-02-D

Eventos de cibersegurança são declarados incidentes com base em critérios estabelecidos

Detalhamento:

Os critérios de declaração de incidentes de cibersegurança estabelecidos são usados para determinar se um evento deve ser declarado incidente. Declarar um incidente inicia as atividades de resposta ao incidente.

E07-RESPOSTA-02-E

Os critérios de declaração de incidentes de cibersegurança são atualizados periodicamente e de acordo com gatilhos definidos, como mudanças organizacionais, lições aprendidas com a execução do plano ou ameaças recém-identificadas

Detalhamento:

Para maximizar o investimento no processo de detecção e resposta a incidentes, os critérios de declaração de incidentes devem ser mantidos para refletir a tolerância ao risco e o ambiente de ameaça em evolução da <Instituição>.

Além disso, atualizar os critérios com base nas lições aprendidas nesse processo pode ajudar a <Instituição> a ser mais eficiente e eficaz ao lidar com eventos futuros.

E07-RESPOSTA-02-F

Existe um repositório onde eventos e incidentes de cibersegurança são documentados e rastreados até o fechamento

Detalhamento:

Documentar e acompanhar garante que um incidente esteja progredindo corretamente ao longo do ciclo de vida do incidente e, mais importante, seja encerrado quando uma resposta adequada e uma revisão pós-incidente forem concluídas.

E07-RESPOSTA-02-G

Partes interessadas internas e externas (por exemplo, executivos, advogados, agências governamentais, <Instituições> conectadas, fornecedores, <Instituições> setoriais, reguladores) são identificadas e notificadas sobre incidentes com base nos requisitos de relatórios de conscientização situacional

Detalhamento:

Incidentes que foram declarados e que exigem uma resposta devem ser comunicados às partes interessadas cujo envolvimento é necessário na implementação, gestão e encerramento de uma solução adequada e rápida.

A notificação de eventos e incidentes deve ser guiada pelos requisitos de reporte definidos na SITUAÇÃO-3d. Mal-entendidos ou informações imprecisas sobre incidentes organizacionais podem ter efeitos graves que superam em muito o potencial de dano causado pelo próprio incidente. Portanto,

a <Instituição> deve gerenciar proativamente as comunicações quando incidentes são detectados e ao longo de seu ciclo de vida.

E07-RESPOSTA-02-H

Os critérios para a declaração de incidentes de cibersegurança estão alinhados com os critérios de priorização de risco cibernético

Detalhamento:

Alinhar os critérios de declaração de incidentes com os critérios de risco estabelecidos no RISCO-3b garante que a <Instituição> reconheça e aborde incidentes que envolvam riscos que a preocupam particularmente.

E07-RESPOSTA-02-I

Incidentes de cibersegurança são correlacionados para identificar padrões, tendências e outras características comuns em múltiplos incidentes

Detalhamento:

A correlação de incidentes pode ser feita por meio de análise, ferramentas de rastreamento de incidentes, uso de categorias de incidentes e correspondência de termos em logs. Por exemplo, logs de acesso ao sistema podem ser verificados para falhas de autenticação do sistema, e os endereços IP desses podem ser correlacionados com endereços IP maliciosos conhecidos coletados por fontes de inteligência.

E07-RESPOSTA-03

Responder a ciberincidentes

E07-RESPOSTA-03-A

O pessoal de resposta a incidentes de cibersegurança é identificado e as funções são atribuídas, pelo menos de forma pontual

Detalhamento:

Identifique os papéis e responsabilidades necessários para realizar atividades de resposta a incidentes de cibersegurança e garanta que os funcionários sejam designados para essas funções e possuam as habilidades necessárias. Os funcionários devem ter autonomia e autoridade suficientes para desempenhar suas funções. a <Instituição> pode criar descrições de cargos para funções e responsabilidades de resposta a incidentes de cibersegurança e acompanhar lacunas de habilidades e lacunas na disponibilidade de funcionários, para que o pessoal adequado possa ser contratado conforme necessário.

E07-RESPOSTA-03-B

Respostas a incidentes de cibersegurança são executadas, para limitar o impacto na função e restaurar as operações normais

Detalhamento:

Responder a um incidente descreve as ações que a <Instituição> toma para prevenir ou conter o impacto de um incidente enquanto ele está ocorrendo ou logo após ter ocorrido. A alcance, o escopo e a amplitude da resposta variarão amplamente dependendo da natureza do incidente. Isso pode incluir

incidentes potenciais que podem ocorrer devido a novas vulnerabilidades ou avanços tecnológicos que têm um impacto significativo na <Instituição>, como vulnerabilidades em tecnologias comumente usadas (por exemplo, MS17-010) e tecnologias emergentes que reduziriam a eficácia dos controles atuais de cibersegurança (por exemplo, computação quântica). A resposta a incidentes pode ser tão simples quanto notificar os usuários para evitar abrir um tipo específico de mensagem de e-mail ou tão complicada quanto a necessidade de implementar planos de continuidade de serviço que exigem a realocação de serviços e operações para um provedor externo.

As ações relacionadas à resposta a incidentes podem incluir, por exemplo, conter danos (por exemplo, desativando hardware ou sistemas), comunicar aos proprietários de ativos sobre o incidente e desenvolver e implementar ações e controles corretivos.

E07-RESPOSTA-03-C

A reportagem de incidentes é realizada (por exemplo, relatórios internos, ICS-CERT, ISACs relevantes)

Detalhamento:

A equipe de resposta a incidentes de cibersegurança deve saber quais informações do incidente devem ser reportadas a diversos stakeholders internos e externos, dentro de qual prazo e se existem restrições (como revisão legal das informações a serem compartilhadas). Sempre que possível, atribua a uma única pessoa a responsabilidade de relatar um incidente durante toda a sua duração para manter as mensagens consistentes à medida que o evento evolui. Mantenha as informações de contato das partes interessadas atualizadas. Os stakeholders podem incluir pessoal, como membros da equipe de relações públicas ou representantes legais, que não estão envolvidos na resposta direta a um incidente, mas devem ser informados para apoiar a manutenção das operações organizacionais.

E07-RESPOSTA-03-D

Planos de resposta a incidentes de cibersegurança que abrangem todas as fases do ciclo de vida do incidente são estabelecidos e mantidos

Detalhamento:

A <Instituição> deve criar um plano bem estruturado e abrangente descrevendo procedimentos de gestão de incidentes, para que as atividades de resposta sejam repetíveis, sejam realizadas com o mesmo nível de rigor em momentos de estresse e tenham resultados consistentes. a <Instituição> pode querer consultar orientações existentes ou especialistas externos para obter informações sobre as melhores <Ações> de gestão de incidentes.

Estes são exemplos de atividades de resposta a incidentes que podem ser descritas no plano:

• Contendo danos;

• Coleta de evidências;

• Comunicando-se com as partes interessadas, incluindo proprietários de ativos e proprietários de incidentes;

• Comunicação com membros da equipe de resposta - incluindo métodos de comunicação de backup ou fora da banda;

• Desenvolver e implementar ações e controles corretivos;

• Implementar planos de continuidade e restauração ou outras ações emergenciais;

• Realizar revisões de lições aprendidas;

• Os tipos de ações que devem ser evitadas durante a resposta.

As atividades devem ser incluídas no plano para todas as fases do ciclo de vida do incidente (por exemplo, triagem, escalonamento, manuseio, comunicação, coordenação e fechamento). Os planos de resposta a incidentes devem ser abrangentes o suficiente para abordar as categorias de incidentes de alto nível que podem afetar a <Instituição>. Os planos de resposta a incidentes também devem abordar possíveis incidentes que possam ocorrer devido a novas vulnerabilidades ou avanços tecnológicos que tenham impacto significativo na <Instituição>, como vulnerabilidades em tecnologias comumente usadas (por exemplo, MS17-010) e tecnologias emergentes que reduziriam a eficácia dos controles atuais de cibersegurança (por exemplo, computação quântica).

Como parte do planejamento de resposta a incidentes, a <Instituição> pode considerar quais acordos legais podem ser necessários em diferentes tipos de cenários de resposta (por exemplo, autorização para que um funcionário federal revise um sistema ou acordos relacionados à obtenção de assistência de uma <Instituição> externa) e se realizar uma revisão jurídica prévia é justificável.

Além disso, à medida que a tecnologia usada para realizar atividades operacionais continua a evoluir para opções mais dispersas e móveis, a <Instituição> pode considerar se os ativos envolvidos em um incidente estarão fisicamente disponíveis durante a resposta e quais capacidades de resposta remota podem ser necessárias.

E07-RESPOSTA-03-E

A resposta a incidentes de cibersegurança é executada de acordo com planos e procedimentos definidos

Detalhamento:

A <Instituição> deve executar a resposta a incidentes com base nos planos e procedimentos definidos. Isso pode incluir responder a incidentes reais ou possíveis incidentes devido a vulnerabilidades graves.

A <Instituição> deve considerar se recursos adequados estarão disponíveis para desempenhar os papéis identificados no plano. Isso pode exigir o envolvimento com outros antes de um incidente para desenvolver pedidos de assistência técnica com autoridades policiais e entidades governamentais, acordos de ajuda mútua com uma <Instituição> parceira, ou contratos e contratos com fornecedores. Esses acordos podem ser preparados antecipadamente para permitir ativação imediata quando for necessária resposta.

Além disso, pode ser útil pré-autorizar o acesso para pessoas que fornecem resposta, a fim de evitar atrasos que possam ser causados por provisão de acesso e treinamentos obrigatórios.

Após a conclusão da resposta a um incidente, a <Instituição> deve realizar revisões ou avaliações para determinar se os planos e procedimentos definidos estão sendo seguidos de forma eficaz.

E07-RESPOSTA-03-F

Os planos de resposta a incidentes de cibersegurança incluem um plano de comunicação para partes interessadas internas e externas

Detalhamento:

As atividades de resposta a incidentes de cibersegurança podem exigir o envolvimento de partes interessadas de toda a <Instituição>, como membros da equipe de relações públicas e representantes legais. Esses stakeholders podem apoiar atividades para mitigar possíveis danos reputacionais durante e após a resposta a um incidente de cibersegurança. a <Instituição> deve considerar os tipos de

comunicação que podem ser necessários para manter as partes interessadas internas e externas informadas durante as atividades de recuperação; por exemplo, executivos e equipes de gestão podem precisar ser informados se ações específicas forem executadas ou se a equipe de resposta a incidentes determinar que um incidente pode causar danos à reputação da <Instituição>.

Esteja ciente de que A <Instituição> frequentemente possuem um plano de comunicação em crises, separado e distinto dos planos de resposta a incidentes de cibersegurança. Nesse caso, o plano de resposta a incidentes de cibersegurança deve fazer referência e utilizar o processo definido no plano de comunicação de crise ao executar comunicações de incidentes para partes interessadas internas e externas.

E07-RESPOSTA-03-G

Os exercícios de plano de resposta a incidentes de cibersegurança são realizados periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

Um planejamento avançado adequado pode ajudar uma <Instituição> a estabelecer, documentar e equipar uma capacidade de gerenciamento de incidentes. Exercícios que desafiem a viabilidade, precisão e completude de um plano de resposta a incidentes devem fazer parte do processo de planejamento. Os exercícios devem ser realizados sob condições e frequência estabelecidas pela <Instituição>. Exercícios baseados em cenários que abrangem múltiplos tipos de cenários e incluem crises externas (por exemplo, enchentes ou pandemias) podem ser úteis para descobrir impactos inesperados em cibersegurança que não decorrem de incidentes de cibersegurança. Os resultados dos exercícios devem ser documentados, juntamente com qualquer informação relevante sobre o nível de preparação da <Instituição> para lidar com incidentes.

Ao planejar exercícios, a <Instituição> deve considerar a coordenação com partes interessadas apropriadas (incluindo terceiros ou fornecedores) para os diferentes tipos de ativos de informação, TI que podem estar dentro do escopo de exercícios como ativos virtualizados, ativos regulados, ativos em nuvem e ativos móveis. Uma dependência significativa de fornecedores durante operações em regime estacionário pode indicar uma necessidade aumentada de suporte de fornecedores durante a resposta a incidentes.

Além disso, os exercícios oferecem uma oportunidade para identificar e comunicar os tipos de ações que devem ser evitadas durante a resposta.

Por fim, a <Instituição> pode considerar o exercício de exceções às políticas e procedimentos normais incluindo exceções como parte do script do cenário de exercício.

E07-RESPOSTA-03-H

Atividades aprendidas de lições aprendidas em incidentes de cibersegurança são realizadas e ações corretivas são tomadas, incluindo atualizações no plano de resposta a incidentes

Detalhamento:

Defina e implemente atividades para coletar informações aprendidas de participantes de resposta a incidentes após incidentes significativos, como sessões hotwash ou envio de comentários em uma wiki da equipe. Os participantes poderiam fornecer feedback sobre o quão bem o plano de resposta a incidentes foi seguido, quaisquer deficiências nos recursos necessários e, de modo geral, quais ações de resposta a incidentes funcionaram bem e quais não. Faça atualizações no plano de resposta a incidentes com base nas lições aprendidas, quando apropriado.

Note que o termo lições aprendidas é usado no sentido comum, geral, e não relacionado a definições usadas em qualquer regulamento ou diretriz específica.

E07-RESPOSTA-03-I

É realizada uma análise da causa raiz dos incidentes de cibersegurança e são tomadas ações corretivas, incluindo atualizações no plano de resposta a incidentes

Detalhamento:

Isso pode envolver a realização de um exame formal das causas do incidente, das formas como a <Instituição> respondeu a ele e das fraquezas administrativas, técnicas e físicas de controle que podem ter permitido que o incidente ocorresse. a <Instituição> pode empregar técnicas comumente disponíveis (como diagramas de causa e efeito) para realizar análises de causa raiz como meio de potencialmente prevenir incidentes futuros de tipo e impacto semelhantes. Quaisquer melhorias necessárias identificadas por essas atividades devem ser feitas, como atualizar o plano de resposta a incidentes ou ajustar estratégias e controles de proteção. Esse tipo de análise pode identificar questões de nível mais alto dentro da <Instituição> e resultar em mudanças em atividades em outros <Eixos>, como a estratégia de risco cibernético, procedimentos de gestão de vulnerabilidades ou o processo de análise de ameaças.

Note que os termos análise da causa raiz e ação corretiva são usados no sentido comum, geral, e não relacionados a definições usadas em qualquer regulamentação ou diretriz específica.

Exceções às políticas implementadas durante a resposta a um incidente devem ser revisadas após a recuperação para seu impacto no ambiente de controle de cibersegurança (ou seja, a transferência das operações do centro de controle apenas do local para remotamente).

Os procedimentos para gerenciar exceções devem incluir requisitos para avaliar mudanças após o retorno às operações normais, incluindo se as mudanças devem permanecer em vigor. Uma análise adicional pode ser valiosa para tipos específicos de alteração, como novos dispositivos, novas aplicações e alterações nas permissões de acesso.

E07-RESPOSTA-03-J

As respostas a incidentes de cibersegurança são coordenadas com fornecedores, autoridades policiais e outras entidades externas, conforme apropriado, incluindo suporte para coleta e preservação de evidências

Detalhamento:

Um evento pode se tornar um incidente organizacional que pode violar as regras, leis e regulamentos locais, estaduais ou federais. Isso geralmente não é conhecido no início da investigação de um evento, por isso a <Instituição> deve estar vigilante para garantir que todas as provas de eventos e incidentes sejam tratadas adequadamente caso uma eventual questão legal, civil ou criminal, seja levantada.

Para coletar, documentar e preservar adequadamente as evidências, a <Instituição> deve ter processos para essas atividades, e esses processos devem ser conhecidos por todos os funcionários envolvidos em qualquer aspecto do ciclo de vida do incidente. Como é imprevisível se um evento ou incidente resultará em ação legal, uma <Instituição> também deve considerar o envolvimento precoce de profissionais jurídicos e possivelmente de aplicação da lei no processo de identificação e análise do incidente para evitar problemas com retenção de provas, destruição e adulteração.

Note que "outras entidades externas" podem incluir terceiros, como provedores de recursos em nuvem.

E07-RESPOSTA-03-K

O pessoal de resposta a incidentes de cibersegurança participa de exercícios conjuntos de cibersegurança com outras organizações

Detalhamento:

Se possível, os profissionais de resposta a incidentes devem participar de exercícios conjuntos de cibersegurança para se familiarizar com as entidades e indivíduos com quem precisariam trabalhar em um incidente real, adquirir experiência em atividades de resposta, possivelmente identificar deficiências nos planos internos de resposta e compartilhar seu conhecimento e experiência com outros membros da comunidade. Um exemplo de exercício conjunto no setor elétrico é o Exercício de Segurança da Rede (GridEx), o exercício anual de dois dias do Departamento de Energia.

E07-RESPOSTA-03-L

Respostas a incidentes de cibersegurança aproveitam e acionam estados de operação predefinidos

Detalhamento:

Uma resposta eficaz exige um planejamento detalhado e antecipado para uma variedade de ameaças e incidentes potenciais. O <Eixo> SITUAÇÃO define "estados de operação pré-definidos" e descreve como eles podem ser usados para garantir que as respostas sejam específicas, medidas e apropriadas para o nível de impacto operacional do incidente. Um exemplo típico dessa abordagem é ter um plano para minimizar o uso da rede em sistemas críticos no caso de serviço de rede degradado. Outro exemplo é ter um plano de ação pronto para mudar para um estado bom conhecido se ficar evidente que seus dados operacionais críticos foram corrompidos.

E08-RESILIÊNCIA

Continuidade de Operações

Resumo:

Considera o planejamento de formas de continuidade das operações mesmo em condições degradadas, incluindo o planejamento prévio da priorização da prestação do serviço em diferentes graus de degradação.

Detalhamento:

O planejamento da continuidade envolve as <Ações> necessárias para sustentar a função em caso de interrupção (parcial ou total) de serviços, como em decorrência de um incidente grave de cibersegurança ou um desastre. Garantir que os planos de continuidade abordem possíveis ciberincidentes requer consideração dos impactos potenciais dos ciberincidentes e das lições aprendidas com incidentes anteriores. Planos de continuidade devem ser testados, e os testes devem incluir cenários de ciberincidentes para garantir que os planos funcionem conforme o esperado durante tais incidentes.

E08-RESILIÊNCIA-01

Abordar a cibersegurança na continuidade das operações

E08-RESILIÊNCIA-01-A

Planos de continuidade são desenvolvidos para sustentar e restaurar a operação da <Instituição> caso ocorra um evento ou incidente de cibersegurança

Detalhamento:

Planos de continuidade contêm descrições das ações que a <Instituição> tomará para sustentar e restaurar a operação da <Instituição> caso ocorra uma interrupção (como falhar para instalações redundantes ou iniciar procedimentos manuais) e papéis-chave que devem estar envolvidos. Geralmente, eles focam em gerenciar as consequências organizacionais da interrupção com base em uma variedade de eventos potenciais que podem causar perturbação. Os planos de continuidade abordam as funções de negócios mais críticas da <Instituição> para garantir que elas continuem durante diferentes tipos de emergências. A <Instituição> também podem considerar como o desligamento seguro será realizado como parte do planejamento de continuidade.

E08-RESILIÊNCIA-01-B

Backups de dados estão disponíveis e testados

Detalhamento:

Esta <Ação> é fundamental para restaurar operações em caso de perda de dados ou falha de hardware. A <Instituição> disponibiliza, backups de ativos de informação. Ao identificar ativos de informação a serem copiados, a <Instituição> deve considerar dados que residem em diferentes tipos de ativos de TI, como ativos virtualizados, ativos regulados, ativos em nuvem, ativos BYOD, ativos gerenciados por terceiros, ativos de campo e ativos móveis. Testes são realizados para backups para ajudar a garantir que eles sejam viáveis e disponíveis quando necessário. As estratégias para realizar e gerenciar backups devem ser baseadas no risco para a <Instituição> ou para a <Instituição>. Esta <Ação> inicia uma progressão de <Ações> que continuam no MIL2 e são focadas em backups de dados.

Backups dos ativos de informação podem incluir:

• Dados operacionais

• Pontos de ajuste

• Arquivos de configuração

• Locais de armazenamento

• Cópias de linhas de base importantes de configuração, imagens douradas, imagens de disco rígido e imagens de máquinas virtuais

Os procedimentos de backup tipicamente incluem:

• Padrões de frequência

• Períodos de retenção

• Locais e métodos autorizados de armazenamento

• Requisitos de criptografia e proteção; padrões de teste

E08-RESILIÊNCIA-01-C

Ativos de TI que precisam de peças sobressalentes são identificados

Detalhamento:

Esta <Ação> é fundamental para restaurar operações em caso de perda ou falha de ativos. a <Instituição> identifica, ativos de TI para os quais podem ser necessários revendas. Esta <Ação> inicia uma progressão de <Ações> que continuam no MIL2 e são focadas em ativos sobressalentes ou redundantes

. Estes são exemplos de ativos de TI sobrantes ou redundantes:

• Switches

• Roteadores

• Controladores

• Sensores

• Ativos virtualizados

• Sistemas dos quais os ativos dependem, como redes de comunicação

E08-RESILIÊNCIA-01-D

Planos de continuidade abordam os impactos potenciais de incidentes de cibersegurança

Detalhamento:

Os planos de continuidade abordam as funções de negócios mais críticas da <Instituição> para garantir que elas continuem durante diferentes tipos de emergências. Portanto, para ajudar a garantir que os planos de continuidade cubram todas as ações que precisam ser tomadas quando certos tipos de incidentes cibernéticos ocorrerem, identifique os tipos que podem realisticamente acontecer com sua <Instituição> e causar uma perturbação significativa. As fontes de informação podem incluir perfis de ameaças, incidentes passados, tendências atuais de ataques, informações sobre vulnerabilidades e alertas de cibersegurança. Técnicas de análise como pesquisa, brainstorming, entrevistas com especialistas no assunto e modelagem de ameaças podem então ser aplicadas para identificar os impactos prováveis desses incidentes. As descrições de impacto devem nomear ativos específicos que

seriam afetados por cada tipo de incidente. Desenvolver tantos planos de continuidade quanto necessário para descrever as ações que precisariam ser tomadas para lidar com possíveis impactos e manter as operações durante a interrupção.

E08-RESILIÊNCIA-01-E

Os ativos e atividades necessários para sustentar as operações mínimas da <Instituição> são identificados e documentados em planos de continuidade

Detalhamento:

Embora A <Instituição> realizem muitas atividades em apoio e relacionadas à execução da <Instituição>, durante períodos de interrupção operações mínimas podem frequentemente ser realizadas com um conjunto menor dessas atividades. Ao identificar o subconjunto de atividades críticas necessárias para apoiar operações mínimas, a <Instituição> pode priorizar as atividades de resposta e concentrar recursos na restauração dos ativos que sustentam essas atividades primeiro.

Os líderes de função devem primeiro decidir o que constitui "operações mínimas". Eles podem fazer isso identificando as operações que afetam mais diretamente a capacidade de alcançar a missão principal da <Instituição>, ou quais operações dependem seus clientes de maior prioridade. As equipes de TI e operações de TO devem então identificar quais sistemas, tecnologias, dados, equipe e processos estão associados à manutenção dessas operações em funcionalidade normal (incluindo quaisquer dependências de funções ou entidades externas). As equipes de TI podem então determinar como operações mínimas podem ser sustentadas em diferentes tipos de condições degradadas (por exemplo, se certos bancos de dados, funcionários ou feeds de dados externos dos quais as operações dependem não estiverem disponíveis).

Além disso, a <Instituição> deve considerar o que a manutenção das operações mínimas pode exigir em diferentes situações. Por exemplo, em uma situação pandêmica em que o trabalho remoto e disseminado é necessário, os indivíduos podem não ter acesso físico a equipamentos de alta prioridade.

E08-RESILIÊNCIA-01-F

Os planos de continuidade abordam ativos de TI, TO e informação que são importantes para a entrega da <Instituição>, incluindo a disponibilidade de dados de backup e ativos de TI de substituição, redundantes e sobressalentes

Detalhamento:

Desenvolvedores de planos de continuidade devem aproveitar informações de inventário e priorização de ativos para garantir que os planos de continuidade cubram todos os ativos importantes para a execução da <Instituição>. Detalhes sobre backups e sobressalentes desses ativos devem ser incluídos nos planos, incluindo backups virtualizados de ativos e snapshots capturados para fins de recuperação. Uma <Instituição> que dependa de uma nuvem como local de backup, seja para dados on-premise ou dados na nuvem, deve considerar o impacto de um evento, incidente ou vulnerabilidade na nuvem na disponibilidade de backups.

E08-RESILIÊNCIA-01-G

Os objetivos de tempo de recuperação (RTOs) e os objetivos de pontos de recuperação (RPOs) para ativos importantes para a entrega da <Instituição> são incorporados aos planos de continuidade

Detalhamento:

Planos de continuidade devem incluir informações para permitir a priorização dos ativos para recuperação em um incidente. Os fatores para o desenvolvimento de RTOs e RPOs incluem o custo de recuperação de um incidente, o custo potencial de inatividade ou perda de dados, requisitos regulatórios, requisitos operacionais e custo da solução de recuperação. Quando RTOs e RPOs foram definidos para quaisquer ativos importantes para a entrega da <Instituição>, eles devem ser incluídos em quaisquer planos de continuidade que contenham etapas de recuperação desses ativos.

E08-RESILIÊNCIA-01-H

Os critérios de incidentes de cibersegurança que acionam a execução dos planos de continuidade são estabelecidos e comunicados ao pessoal de resposta a incidentes e gestão de continuidade

Detalhamento:

Deve ser estabelecida uma ligação entre a resposta a incidentes e as atividades de continuidade. Determine as condições sob as quais um plano de continuidade deve ser executado e garanta que o pessoal de resposta a incidentes e os proprietários dos planos de continuidade compreendam essas condições.

E08-RESILIÊNCIA-01-I

Os planos de continuidade são testados periodicamente por meio de avaliações e exercícios de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

Os testes são frequentemente a única oportunidade para uma <Instituição> saber se os planos atendem aos seus objetivos declarados. Os testes devem ser realizados em um ambiente controlado. O programa de testes e os padrões devem ser aplicados para garantir consistência e a capacidade de interpretar os resultados no nível organizacional.

Os padrões para testes de continuidade podem incluir:

• Tipos de testes (por exemplo, walkthroughs, mesas, testes de dependência, testes de backup e peças de reposição)

• Componentes de teste exigidos

• Padrões de garantia de qualidade

• Envolvimento e compromisso das partes interessadas do plano

• Padrões de relatórios

• Padrões de medição

• Manutenção do plano de teste

Testes de backup e armazenamento e procedimentos relacionados devem ser feitos para garantir que estejam atendendo aos requisitos da <Instituição>. Testes periódicos dos procedimentos de backup e armazenamento da <Instituição> ajudam a garantir a validade contínua à medida que as condições operacionais mudam.

Além disso, a <Instituição> deve considerar a coordenação com as partes interessadas adequadas para os diferentes tipos de ativos de TI, TO e informação que podem estar dentro do escopo de exercícios como ativos virtualizados, ativos regulados, ativos em nuvem e ativos móveis.

E08-RESILIÊNCIA-01-J

Os controles de cibersegurança que protegem dados de backup são equivalentes ou mais rigorosos do que os controles que protegem dados de origem

Detalhamento:

Certifique-se de que os controles usados para proteger os dados de backup sejam pelo menos equivalentes aos controles que protegem os dados de origem. a <Instituição> deve selecionar controles projetados para atender aos requisitos de cibersegurança. a <Instituição> pode exigir que os dados de backup tenham controles de cibersegurança mais rigorosos, como monitoramento da integridade dos dados ou o uso da tecnologia de gravação uma vez, leia muitos (WORM) para evitar a modificação dos dados.

E08-RESILIÊNCIA-01-K

Backups de dados são separados logica ou fisicamente dos dados de origem

Detalhamento:

Backups de dados são armazenados de forma a reduzir ou eliminar o risco de que um ataque cibernético que resulte em alteração ou destruição dos dados também possa resultar em alteração ou destruição dos backups desses dados.

E08-RESILIÊNCIA-01-L

Peças sobressalentes para ativos selecionados de TI estão disponíveis

Detalhamento:

A <Instituição> disponibiliza ou possui procedimentos para obter ativos de TI extras ou redundantes . Testes e manutenção rotineira (como patches e atualizações de configuração) são realizados para peças de reposição e redundâncias para ajudar a garantir que sejam viáveis e estejam disponíveis quando necessário.

Estes são exemplos de ativos de TI sobrando ou redundantes:

• Switches

• Roteadores

• Controladores

• Sensores

• Ativos

• Virtualizados

• Sistemas nos quais os ativos dependem, como redes de comunicação

E08-RESILIÊNCIA-01-M

Os planos de continuidade são alinhados com os riscos identificados e o perfil de ameaça da <Instituição> para garantir a cobertura das categorias de risco e ameaças identificadas

Detalhamento:

Ao desenvolver planos de continuidade, a <Instituição> deve revisar as categorias de risco e o perfil de ameaça da <Instituição> para ajudar a garantir que planos de continuidade sejam desenvolvidos para todos os tipos potenciais de incidentes cibernéticos. Para alinhar o planejamento de continuidade com o perfil de ameaça, a <Instituição> deve revisar os ativos-alvo, objetivos e métodos de ataque que podem ser empregados por atores de ameaça e ajustar os cenários de continuidade para lidar com os impactos potenciais das ameaças de cibersegurança. Por exemplo, o perfil de ameaça pode descrever um cenário viável em que sistemas de controle de fabricação são comprometidos e malware destrutivo é implantado, causando danos físicos a equipamentos de fabricação especializados. Um plano de continuidade seria desenvolvido que continha todas as ações necessárias para recuperar os sistemas de controle, iniciar o reparo ou substituição dos equipamentos de fabricação afetados e sustentar as operações de manufatura tanto quanto possível durante a interrupção.

E08-RESILIÊNCIA-01-N

Exercícios de plano de continuidade abordam riscos de maior prioridade

Detalhamento:

A <Instituição> deve usar informações sobre riscos priorizados para criar cenários específicos para os quais os planos de continuidade devem ser testados.

E08-RESILIÊNCIA-01-O

Os resultados dos testes ou ativação do plano de continuidade são comparados aos objetivos de recuperação, e os planos são aprimorados de acordo

Detalhamento:

Tanto os testes de planos de continuidade quanto a ativação de planos em incidentes reais podem fornecer insights sobre se os planos funcionam como deveria. Após um teste ou a ativação de um plano, os resultados devem ser comparados com os objetivos de recuperação do plano, incluindo quaisquer RTOs e RPOs definidos. Áreas onde os objetivos não puderam ser atingidos devem ser registradas e estratégias desenvolvidas para revisar e revisar o plano. Melhorias no processo e nos planos de testes também devem ser identificadas, documentadas e incorporadas em testes futuros.

Testes e ativação do plano de continuidade podem revelar melhorias necessárias devido a

• Falta de recursos suficientes

• Falta de recursos adequados

•Lacunas de treinamento para a equipe e partes interessadas do plano

.• Conflitos no plano (se múltiplos planos forem testados simultaneamente)

• Deficiências de infraestrutura

E08-RESILIÊNCIA-01-P

Os planos de continuidade são periodicamente revisados e atualizados

Detalhamento:

O teste e a execução dos planos de continuidade do serviço são duas fontes de potenciais atualizações nos planos. No entanto, um ambiente operacional dinâmico, fontes de novas ameaças e riscos, e

mudanças como as da equipe, localização geográfica e relacionamentos com entidades externas podem exigir alterações nos planos de continuidade do serviço e em seus respectivos planos de teste.

Estes são exemplos de condições que podem resultar em mudanças nos planos de continuidade:

• Identificação de novas vulnerabilidades, ameaças e riscos

• Mudanças em TI, TO ou ativos de informação

/realocação de instalações

/mudanças nos controles de proteção de um ativo

/mudanças nas partes interessadas do plano, incluindo entidades externas e agências públicas

E09-EQUIPE

Gestão da força de trabalho

Resumo:

À medida que as instituições adotam cada vez mais tecnologia digital avançada, é um desafio aprimorar os conjuntos de habilidades de sua força de trabalho existente e contratar pessoal com o nível adequado de experiência, educação e treinamento em cibersegurança. A dependência das instituições em tecnologia avançada para comunicações e controle digital continua a crescer, e os problemas da força de trabalho são um aspecto crucial para abordar com sucesso a cibersegurança e o gerenciamento de riscos para esses sistemas.

Os acordos coletivos de trabalho podem desafiar alguns aspectos das práticas neste <Eixo> conforme escritas, portanto, as instituições podem precisar implementar práticas alternativas que atendam à intenção das práticas modelo e se alinhem a esses acordos.

Detalhamento:

A implementação de controles de equipes (força de trabalho) inclui a verificação de antecedentes de pessoal, procedimentos de desligamento e acordos de uso aceitável. Controles adicionais podem ser apropriados para cargos considerados de maior risco potencial para a <Instituição>, como aqueles que têm acesso a ativos necessários para a prestação de um serviço essencial. Por exemplo, administradores de sistemas geralmente têm a capacidade de alterar configurações, modificar ou excluir arquivos de log, criar contas e alterar senhas em sistemas críticos, e medidas adicionais podem ser necessárias para proteger esses sistemas contra comportamentos acidentais ou maliciosos por parte dessa categoria de pessoal.

Aumentar a conscientização sobre cibersegurança da equipe é tão importante quanto as abordagens tecnológicas para melhorar a cibersegurança da <Instituição>. A ameaça de um ataque cibernético a uma <Instituição> geralmente começa com a obtenção de alguma posição nos sistemas de TI ou TO de uma <Instituição>, por exemplo, ganhando a confiança de um funcionário ou contratado incauto. Funcionários e contratados devem receber treinamento periódico de conscientização de segurança para reduzir sua vulnerabilidade à engenharia social e outras ameaças. A <Instituição> deve compartilhar informações com sua equipe sobre métodos e técnicas para identificar comportamentos suspeitos, evitar spam e spear phishing e reconhecer ataques de engenharia social para evitar fornecer informações sobre a <Instituição> ou divulgar involuntariamente credenciais de login a adversários em potencial. Por exemplo, um site interno pode fornecer informações sobre novas ameaças e vulnerabilidades no setor. Se nenhuma informação sobre ameaças, vulnerabilidades e práticas recomendadas for compartilhada com a força de trabalho, o pessoal pode ficar negligente com os processos e procedimentos de segurança. A eficácia das <Ações> de conscientização sobre cibersegurança deve ser avaliada periodicamente e melhorias devem ser feitas conforme necessário.

A atribuição de responsabilidades de cibersegurança começa com a identificação das principais responsabilidades de cibersegurança necessárias para apoiar as metas operacionais e de gerenciamento de riscos da <Instituição>. As responsabilidades de cibersegurança identificadas podem ser atribuídas a funções de trabalho e documentadas. O planejamento da força de trabalho ajuda a garantir que os recursos adequados estejam disponíveis para cumprir as principais funções da força de trabalho de cibersegurança. As responsabilidades de cibersegurança não se restringem às funções tradicionais de TI. Por exemplo, engenheiros, operadores de sala de controle e técnicos de campo podem ter responsabilidades de cibersegurança.

O desenvolvimento da força de trabalho de cibersegurança inclui treinamento e recrutamento para abordar as lacunas de habilidades identificadas. Por exemplo, os profissionais de recursos humanos

podem reagir às deficiências de habilidades de cibersegurança dentro da <Instituição>, priorizando habilidades específicas de cibersegurança durante a execução de <Ações> de recrutamento e entrevista.

Além disso, o pessoal (e contratados) deve receber treinamento periódico de conscientização de segurança para reduzir sua vulnerabilidade à engenharia social e outras ameaças. A eficácia das <Ações> de treinamento e conscientização deve ser avaliada e melhorias devem ser feitas conforme necessário.

E09-EQUIPE-01

Implementar controles da força de trabalho

E09-EQUIPE-01-A

A triagem de pessoal (por exemplo, verificações de antecedentes, testes de drogas) é realizada na contratação

Detalhamento:

Coordenar com a equipe de Recursos Humanos para garantir que verificações de crédito, antecedentes criminais, testes de drogas, verificação de credenciais e empregos anteriores, e possivelmente outras verificações, sejam realizadas. Em certos casos, você pode aceitar uma verificação recíproca de antecedentes de um empregador anterior (como o governo federal).

Além disso, acompanhe qualquer coisa comunicada por alguém que o candidato tenha dado como referência que levante dúvidas sobre a confiabilidade do candidato. O objetivo é eliminar qualquer evidência ou indicador de que o candidato possa acabar sendo uma ameaça interna (por exemplo, instabilidade financeira, histórico criminal, comportamento suspeito ou disruptivo em empregos anteriores, mentiras).

A triagem pode ser realizada internamente por funcionários de Recursos Humanos ou contratada por um fornecedor, mas em ambos os casos deve ser feita por profissionais que compreendam todas as leis e regulamentos aplicáveis. Para cargos terceirizados, exija que os fornecedores realizem uma verificação equivalente de quaisquer contratados que tenham acesso aos ativos organizacionais.

E09-EQUIPE-01-B

Os procedimentos de separação de pessoal abordam a cibersegurança

Detalhamento:

Garantir que os profissionais que saírem não continuem tendo acesso a ativos, especialmente aqueles que têm acesso privilegiado ou a dados financeiros, PII ou propriedade intelectual. Crie procedimentos para remover, revogar ou desativar o acesso a todos os ativos organizacionais a partir da data de rescisão do funcionário. Comece identificando todas as contas do funcionário (incluindo quaisquer contas que ele tenha com provedores terceirizados, como contas da empresa em instituições financeiras), acesso elevado de qualquer tipo, como administrador ou NERC-CIP, todos os dispositivos em posse do funcionário e todos os sistemas, dados e outros ativos aos quais o funcionário tem acesso. Desative todas as contas, remova o acesso a todos os ativos afetados, remova o acesso remoto e recolha os dispositivos, crachá, tokens, documentos proprietários impressos, cartões de crédito da empresaetc. Coordene com o RH para estabelecer o horário dos eventos e quem é responsável por quê. Para funcionários com acesso privilegiado ou acesso a dados sensíveis, você pode querer monitorar a atividade da rede para identificar qualquer evidência de exfiltração de dados.

Para o pessoal que está sendo demitido involuntariamente, considere remover, revogar ou desativar todo o acesso a ativos imediatamente após informar o funcionário sobre a demissão. Acompanhe o funcionário para fora do local imediatamente após fazer o anúncio. Você também pode querer examinar quaisquer sistemas ou computadores que o funcionário tenha usado para detectar sinais de exfiltração ou comprometimento de dados.

E09-EQUIPE-01-C

A triagem de pessoal é realizada na contratação e periodicamente para cargos que têm acesso a ativos importantes para a execução da <Instituição>

Detalhamento:

Para funcionários que têm acesso privilegiado ou confiável aos ativos, a triagem é realizada não apenas na contratação, mas periodicamente. Fazer isso ajuda a <Instituição> a descobrir se houve alguma mudança no comportamento do funcionário ou se as circunstâncias que possam levantar novas questões de confiança.

E09-EQUIPE-01-D

Procedimentos de separação e transferência de pessoal abordam a cibersegurança, incluindo a verificação suplementar conforme apropriado

Detalhamento:

Riscos potenciais decorrentes da transferência de pessoal devem ser identificados e procedimentos para mitigar esses riscos devem ser estabelecidos e mantidos. Para funcionários que têm acesso privilegiado ou confiável aos ativos, gerenciar o acesso e a posse desses ativos é extremamente importante para evitar possíveis interrupções ou efeitos na resiliência da <Instituição>. Quando o pessoal muda de cargo, sua posse e acesso aos ativos organizacionais (incluindo seus privilégios de acesso) devem ser reavaliados e ajustados conforme necessário. Também pode ser necessário considerar a reatribuição de responsabilidades de cibersegurança. a <Instituição> pode considerar uma avaliação adicional para os funcionários que se transferem para uma nova posição que apresenta maior risco para a <Instituição>.

E09-EQUIPE-01-E

O pessoal é informado sobre suas responsabilidades na proteção e uso aceitável de ativos de TI, TO e informações

Detalhamento:

Funcionários e outros usuários dos ativos de TI, TO e informações da <Instituição> devem ser informados sobre suas próprias responsabilidades para a proteção e o uso aceitável desses ativos. a <Instituição> deve definir métodos para comunicar claramente responsabilidades, como treinamentos periódicos de conscientização sobre segurança e políticas. Por exemplo, uma política de uso aceitável, por exemplo, pode estabelecer os limites dos comportamentos aceitáveis ao usar os sistemas e dados da <Instituição>, como proibir a sincronização e reutilização de senhas entre sistemas ou o uso de cofres pessoais para misturar o gerenciamento tanto de senhas pessoais quanto organizacionais. a <Instituição> pode considerar treinamentos suplementares para usuários que têm acesso a ativos de TI, TO e informações com requisitos de proteção maiores.

Para reforçar as expectativas de proteção necessária para ativos mais sensíveis de TI, TO e informação, a <Instituição> pode considerar criar metas e objetivos para os usuários em torno dos requisitos de proteção desses ativos.

E09-EQUIPE-01-F

A triagem é realizada para todas as posições (incluindo funcionários, fornecedores e contratados) em um nível compatível com o risco da posição

Detalhamento:

A triagem deve ser realizada para todas as posições e em um nível que reflita o risco associado a cada cargo. O nível de risco associado a uma posição pode ser devido ao nível de autoridade (como CEO), nível de responsabilidade (como administrador de rede) ou acesso a ativos com custo, sensibilidade ou criticidade significativa para a <Instituição>.

E09-EQUIPE-01-G

Um processo formal de responsabilização que inclui ações disciplinares é implementado para o pessoal que não cumpre as políticas e procedimentos de segurança estabelecidos

Detalhamento:

Um processo disciplinar é um controle administrativo essencial para a aplicação das políticas de resiliência organizacional. A conscientização sobre o processo disciplinar oferece aos funcionários um incentivo adicional para cumprir as políticas de resiliência da <Instituição> e garante um tratamento justo e adequado caso haja suspeita de irregularidades. Do ponto de vista da <Instituição>, um processo disciplinar formalizado fornece uma resposta pré-planejada para suspeitas de infrações da política de cibersegurança, projetada para abordar todas as preocupações relevantes enquanto protege a <Instituição> ao máximo.

O processo disciplinar deve ser formalizado e documentado. Deve garantir um tratamento justo da equipe em conformidade com todas as regulamentações e acordos aplicáveis, proteger os interesses da <Instituição> e incluir uma variedade de respostas aceitáveis que correspondam à gravidade da infração.

Revise o processo disciplinar conforme necessário.

E09-EQUIPE-02

Aumentar a conscientização sobre cibersegurança

E09-EQUIPE-02-A

Atividades de conscientização em cibersegurança ocorrem

Detalhamento:

Realizar atividades para aprimorar a compreensão dos funcionários sobre riscos cibernéticos, leis e regulamentos relacionados à cibersegurança aos quais a <Instituição> está sujeita, e políticas, procedimentos e requisitos de cibersegurança. Os tópicos podem ser gerais, para todo o pessoal (como reportagem de eventos), ou especificamente para determinados papéis (como riscos de engenharia social que afetam a equipe de serviços financeiros). Todos os funcionários de cibersegurança devem estar cientes da estratégia do programa de cibersegurança, portanto, briefings sobre ela devem ser incluídos nas atividades de conscientização. Algumas comunicações de conscientização podem ser

necessárias com parceiros de negócios, como como a forma como as PII são tratadas e como a conformidade com os padrões é alcançada.

As atividades de conscientização sobre cibersegurança podem incluir e-mails focados em cibersegurança de especialistas reconhecidos, recapitulações trimestrais, sessões de almoço e aprendizado, pôsteres e um site dedicado à intranet onde notícias sobre eventos atuais de cibersegurança e artigos relevantes, memorandos, alertasetc. são publicados.

Estes são exemplos de tópicos de conscientização em cibersegurança: phishing por e-mail e outras táticas de engenharia social; reconhecimento de indicadores de ameaças internas; identificação de eventos e incidentes; classificação e tratamento de dados; políticas de uso aceitável; gestão de identidade, incluindo contas em nuvem; autoridades de contas; conectividade remota; e segurança de dispositivos móveis.

E09-EQUIPE-02-B

Os objetivos de conscientização em cibersegurança são estabelecidos e mantidos

Detalhamento:

Os objetivos das atividades de conscientização em cibersegurança são baseados em necessidades de conscientização que definem as mensagens que precisam ser comunicadas sobre cibersegurança para a equipe e outros atores internos e externos. Para alguns temas, as necessidades de conscientização podem ser consistentes em toda a população da <Instituição> ; Para outros, diferentes partes interessadas podem ter necessidades de conscientização distintas. Todos esses grupos devem ser identificados e suas necessidades de conscientização documentadas.

Fontes de conscientização incluem:

• Requisitos de cibersegurança que especificam como os ativos devem ser protegidos e mantidos; políticas organizacionais que tentam impor e reforçar comportamentos aceitáveis ou implementar controles necessários em toda a empresa, como manter dados de folha de pagamento confidenciais, vulnerabilidades sob vigilância ou que estejam sendo gerenciadas ativamente

• Leis e regulamentos aos quais a <Instituição> está sujeita devido à sua indústria, localização geográfica ou tipo de negócio

• Manter a segurança enquanto utiliza tipos específicos de tecnologia que representam risco cibernético aumentado, como e-mail e dispositivos móveis

As necessidades de conscientização são temporárias e podem mudar como resultado de mudanças na tecnologia, política, estratégia e riscos gerenciados. Um processo rotineiro para manter e atualizar as necessidades de conscientização deve ser implementado.

E09-EQUIPE-02-C

Os objetivos de conscientização em cibersegurança estão alinhados com o perfil de ameaça definido (AMEAÇA-2e)

Detalhamento:

Para alinhar os objetivos de conscientização em cibersegurança com o perfil de ameaça definido, analise o perfil de ameaça para entender os ativos, objetivos e métodos de ataque que podem ser empregados pelos agentes ameaçadores. Isso apoia a identificação dos tipos e da extensão dos esforços de conscientização necessários para enfrentar ameaças relevantes para a <Instituição>. Por exemplo,

se o perfil de ameaça incluir uma ameaça envolvendo spear phishing, pode ser criado conteúdo de conscientização sobre esse tema.

E09-EQUIPE-02-D

Atividades de conscientização sobre cibersegurança são realizadas periodicamente

Detalhamento:

Esta <Ação> se baseia nas atividades de conscientização em cibersegurança para incluir a execução dessas atividades de acordo com períodos definidos organizacionalmente. Por exemplo, isso pode incluir atividades de conscientização exigidas como parte da integração de novos funcionários, bem como atividades anuais de reciclagem.

E09-EQUIPE-02-E

As atividades de conscientização em cibersegurança são adaptadas ao papel profissional

Detalhamento:

As atividades de conscientização em cibersegurança podem ser adaptadas para funções específicas. Por exemplo, treinamentos mais avançados em conscientização em engenharia social podem ser considerados para cargos de maior risco, como liderança organizacional ou cargos que têm autoridade para aprovar transações financeiras.

E09-EQUIPE-02-F

Atividades de conscientização em cibersegurança abordam estados predefinidos de operação

Detalhamento:

Os requisitos de comunicação para conscientização em cibersegurança devem incluir o fornecimento de informações sobre estados predefinidos de operação. Por exemplo, comunicações de conscientização podem incluir informações sobre quando e por que uma mudança do estado normal de operação para um modo operacional de alta segurança pode ser invocada em resposta a um incidente de cibersegurança declarado de gravidade suficiente.

E09-EQUIPE-02-G

A eficácia das atividades de conscientização em cibersegurança é avaliada periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos, e melhorias são feitas conforme apropriado

Detalhamento:

A <Instituição> deve ter um processo documentado para avaliar a eficácia das atividades de conscientização. Normalmente, a avaliação da eficácia é feita fazendo com que os funcionários preencham avaliações após atividades de conscientização. É mais desafiador avaliar a eficácia de outros mecanismos de conscientização, como cartazes ou comunicações regulares.

Estes são exemplos de métodos que podem ser usados para avaliar a eficácia das atividades de conscientização:

• Questionários ou pesquisas projetados para medir a consciência das pessoas sobre tópicos específicos

• Grupos focais para obter o nível de consciência de um grupo após uma atividade de conscientização e para coletar recomendações de melhoria

• Entrevistas seletivas para questionar sobre a conscientização e quaisquer mudanças de comportamento que possam ter ocorrido como resultado das atividades de conscientização

• Medidas comportamentais para avaliar objetivamente mudanças no comportamento após uma atividade de conscientização — por exemplo, avaliar a força das senhas antes e depois de uma atividade de conscientização — observações, avaliações e atividades de benchmarking conduzidas por entidades externas

E09-EQUIPE-03

Atribuir responsabilidades de cibersegurança

E09-EQUIPE-03-A

As responsabilidades de cibersegurança para a <Instituição> são identificadas

Detalhamento:

Identifique os papéis e atividades necessários para atender às necessidades do programa de cibersegurança da <Instituição>. Isso incluiria funções típicas de cibersegurança, como administrador de segurança, administrador de rede e diretor de segurança da informação (ou função similar) e suas atividades atribuídas. As responsabilidades em cibersegurança não se restringem a funções tradicionais de cibersegurança ou TI. Por exemplo, engenheiros de operações, especialistas em recursos humanos e especialistas em compras normalmente ocupam funções de cibersegurança, e essas funções podem ser desempenhadas por terceiros. Pode ser útil considerar as melhores <Ações> ou frameworks do setor de consultoria, como o NICE Cybersecurity Workforce Framework (Publicação Especial 800-181 do NIST) para ajudar na identificação e descrição de responsabilidades fundamentais em cibersegurança.

E09-EQUIPE-03-B

As responsabilidades de cibersegurança são atribuídas a pessoas específicas

Detalhamento:

A <Instituição> deve alocar pessoal às responsabilidades de cibersegurança. Esses podem ser cargos em tempo integral ou apenas um pequeno conjunto de responsabilidades atribuídas a alguém cuja função principal é em outra área. O objetivo principal é garantir que alguma(s) pessoa específica (ou pessoas) seja responsável por cada uma das atividades necessárias para implementar o programa de cibersegurança da <Instituição>.

E09-EQUIPE-03-C

As responsabilidades de cibersegurança são atribuídas a funções específicas, incluindo prestadores de serviços externos

Detalhamento:

Atribuir claramente responsabilidades de cibersegurança aos papéis estabelece expectativas para as tarefas que os profissionais nessas funções realizarão. Esses papéis podem ser explicitamente focados em cibersegurança (administrador de rede, help desk, CISO etc.) ou podem ser outros papéis que contribuem para atividades de cibersegurança. Essas responsabilidades também devem ser especificadas em acordos formais com entidades externas, como provedores de serviços de Internet,

provedores de segurança como provedores de serviços, provedores de serviços em nuvem e provedores de serviços de TI/TO.

E09-EQUIPE-03-D

As responsabilidades em cibersegurança estão documentadas

Detalhamento:

As responsabilidades em cibersegurança devem ser claramente documentadas (em descrições de cargos ou critérios de desempenho, por exemplo) para que os membros da equipe conheçam suas responsabilidades e possam planejar seu desempenho de acordo. A definição de responsabilidades em cibersegurança na descrição do cargo estabelece a base para a gestão de desempenho e a medição do compromisso do membro da equipe em ajudar a <Instituição> a manter a resiliência operacional.

E09-EQUIPE-03-E

As responsabilidades e requisitos de trabalho em cibersegurança são revisados e atualizados periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e na estrutura organizacional

Detalhamento:

As responsabilidades e requisitos de um cargo devem ser revisados e atualizados de forma predeterminada, usando um ou mais gatilhos, como tempo decorrido, mudanças de pessoal e mudanças de processo. Esses gatilhos garantem que as responsabilidades e requisitos do cargo se adaptem a mudanças no risco organizacional, nos processos organizacionais ou no cenário de ameaças. Manter as responsabilidades e requisitos do cargo atualizados ajuda a garantir que os funcionários tenham uma compreensão clara dos papéis que desempenham na cibersegurança da <Instituição>.

E09-EQUIPE-03-F

As responsabilidades atribuídas em cibersegurança são gerenciadas para garantir a adequação e redundância da cobertura, incluindo o planejamento sucessório

Detalhamento:

O planejamento e a análise de recursos devem ser realizados para determinar os requisitos de pessoal para atividades de cibersegurança. O orçamento periódico deve garantir financiamento adequado para esses requisitos. As necessidades de pessoal devem incluir treinamento e disponibilidade de pessoal de reserva, pelo menos para tarefas críticas. O planejamento sucessório deve envolver gestores de nível superior para identificar potenciais sucessores e garantir que sejam orientados e treinados para assumir cargos futuros, dependendo de vagas que ainda não tenham ocorrido.

E09-EQUIPE-04

Desenvolver a força de trabalho de cibersegurança

E09-EQUIPE-04-A

O treinamento em cibersegurança é disponibilizado para profissionais com responsabilidades de cibersegurança atribuídas

Detalhamento:

Garantir que o pessoal com responsabilidades designadas tenha o conhecimento e as habilidades necessárias para desempenhar essas responsabilidades. Realize treinamento em cibersegurança internamente ou inclua financiamento no orçamento do programa de cibersegurança para que os funcionários possam fazer treinamento com fornecedores. Se o treinamento for fornecido internamente, ele deve ser relevante para os tipos de atividades identificadas.

Além disso, as responsabilidades de cibersegurança não se restringem a funções tradicionais de cibersegurança ou TI. Por exemplo, engenheiros de operações, especialistas em recursos humanos e especialistas em compras normalmente ocupam funções de cibersegurança, e essas funções podem ser desempenhadas por terceiros.

O treinamento pode incluir a participação em conferências que oferecem sessões aprofundadas, treinamentos específicos para fornecedores sobre ferramentas usadas e programas de certificação. O pagamento por treinamentos externos e programas de certificação pode ser feito apenas com base de reembolso após a conclusão bem-sucedida.

E09-EQUIPE-04-B

Os requisitos e lacunas de conhecimento, habilidades e capacidades em cibersegurança são identificados tanto para necessidades operacionais atuais quanto futuras

Detalhamento:

Para identificar lacunas, você pode primeiro criar um inventário de habilidades para identificar e documentar o conjunto atual de habilidades do pessoal da <Instituição>. Esse inventário oferece um panorama das capacidades atuais e pode ser usado para diagnosticar escassez e lacunas de recursos tanto em relação às suas necessidades atuais quanto futuras da sua força de trabalho.

O inventário de habilidades é comparado com as responsabilidades identificadas em cibersegurança para a <Instituição> para identificar habilidades que a <Instituição> não possui. A lacuna de habilidades resultante fornece uma visão sobre as necessidades atuais e futuras da <Instituição>. Essas lacunas de habilidades podem impedir que a <Instituição> desse desempenho adequado na gestão dos riscos cibernéticos e podem resultar em riscos adicionais.

E09-EQUIPE-04-C

As lacunas identificadas de conhecimento, habilidades e habilidades em cibersegurança são abordadas por meio de treinamento, recrutamento e esforços de retenção

Detalhamento:

uma <Instituição> pode abordar lacunas de conhecimento e habilidades de várias maneiras: funcionários existentes podem ser treinados para adquirir novas habilidades, novos funcionários podem ser contratados para adquirir as necessárias, ou as habilidades podem ser adquiridas terceirizando o trabalho que as exige. À medida que lacunas são preenchidas, o inventário de habilidades deve ser atualizado para garantir que os esforços de recrutamento e treinamento estejam alinhados às necessidades atuais.

E09-EQUIPE-04-D

O treinamento em cibersegurança é fornecido como pré-requisito para conceder acesso a ativos importantes para a execução da <Instituição>

Detalhamento:

Novos profissionais e transferidos para novas posições são treinados em princípios, requisitos e melhores <Ações> de cibersegurança antes de terem acesso a TI, TO e ativos de informação. O treinamento pode incluir treinamento em cibersegurança específico para as responsabilidades da posição ou para os ativos acessados na posição (como treinamento em segurança da cadeia de suprimentos ou segurança em nuvem), além de treinamento geral em cibersegurança que se aplica a todo o pessoal.

E09-EQUIPE-04-E

A eficácia dos programas de treinamento é avaliada periodicamente, e melhorias são feitas conforme apropriado

Detalhamento:

Deve existir um processo para determinar a eficácia do treinamento para atender às necessidades de treinamento dos funcionários envolvidos no programa de cibersegurança.

Estes são exemplos de métodos usados para avaliar a eficácia do treinamento:

• Testes no contexto do treinamento

• Pesquisas pós-treinamento com participantes do treinamento

• Pesquisas pós-treinamento com gestores dos participantes sobre sua satisfação com o impacto do treinamento na capacidade dos participantes de desempenhar suas responsabilidades em cibersegurança

• Mecanismos de avaliação embutidos nos materiais de treinamento

Documente melhorias sugeridas no plano de treinamento com base na avaliação da eficácia das atividades de treinamento e implemente melhorias quando possível.

E09-EQUIPE-04-F

Os programas de treinamento incluem educação continuada e oportunidades de desenvolvimento profissional para profissionais com responsabilidades significativas em cibersegurança

Detalhamento:

A ampla gama de habilidades necessárias para desempenhar adequadamente as competências exigidas no programa de cibersegurança exige treinamento extensivo e contínuo. Devido à natureza crítica dessas responsabilidades do programa, é importante que as oportunidades para que o pessoal de cibersegurança receba treinamento seja planejada e orçamentada.

E10-TERCEIROS

Gestão de Riscos de Terceiros

Resumo:

À medida que as interdependências entre infraestruturas, parceiros operacionais, fornecedores e prestadores de serviços aumentam, estabelecer e manter uma compreensão abrangente dos principais relacionamentos e gerenciar seus ciber-riscos associados é essencial para a entrega segura, confiável e resiliente da função.

Detalhamento:

A identificação de terceiros envolve estabelecer e manter uma compreensão abrangente dos principais relacionamentos externos necessários para a entrega da função. Após a identificação, os terceiros devem ser priorizados para determinar quais dependências de terceiros são mais críticas para a entrega da função. Os critérios de priorização devem considerar o risco para a função que é introduzido por relacionamentos com terceiros.

O modelo classifica as dependências de terceiros como partes externas das quais a entrega da função depende, incluindo parceiros operacionais. Esses relacionamentos podem variar em importância, pois a função pode ter uma dependência maior de terceiros específicos, principalmente se um terceiro tiver acesso, controle ou custódia de um ativo. Terceiros incluem entidades como fornecedores, vendedores, prestadores de serviços, dependências de infraestrutura (por exemplo, telecomunicações, água) e instituições governamentais (por exemplo, serviços de resposta a emergências, parceiros federais).

O risco na cadeia de suprimentos é um exemplo notável de dependência de fornecedores. As características de cibersegurança de produtos e serviços variam amplamente. Sem uma gestão de riscos adequada, representam sérias ameaças, incluindo software de origem desconhecida e hardware falsificado (possivelmente malicioso).

As solicitações de propostas das instituições frequentemente fornecem aos fornecedores de sistemas, dispositivos e serviços de alta tecnologia apenas especificações vagas, que podem não atender aos requisitos adequados de segurança, garantia de qualidade e disponibilidade. A autonomia que as instituições costumam conceder às suas unidades de negócios individuais aumenta ainda mais o risco, a menos que as <Ações> de contratação e compra sejam limitadas por um plano ou política para incluir requisitos de cibersegurança.O gerenciamento de riscos de terceiros inclui abordagens como testes independentes, revisão de código, verificação de vulnerabilidades e revisão de evidências demonstráveis do fornecedor de que um processo seguro de desenvolvimento de software foi seguido. Os contratos que vinculam a <Instituição> a um relacionamento com um parceiro ou fornecedor de produtos ou serviços devem ser revisados para determinar a adequação dos requisitos relacionados ao ciber-risco, como a linguagem do contrato que estabelece as responsabilidades do fornecedor por atender ou exceder os padrões ou diretrizes de cibersegurança especificados. Os contratos de nível de serviço podem especificar processos de monitoramento e auditoria para verificar se fornecedores e provedores de serviços atendem à cibersegurança e outras medidas de desempenho.

E10-TERCEIROS-01

Identificar e priorizar terceiros

E10-TERCEIROS-01-A

Dependências importantes de terceiros de TI são identificadas (ou seja, partes internas e externas das quais depende a entrega da <Instituição>, incluindo parceiros operacionais)

Detalhamento:

Identificar e manter informações básicas sobre partes internas e externas que possam ser necessárias para a continuidade do desempenho da <Instituição>. Dependências de fornecedores, por exemplo, podem incluir provedores de serviços de TI, consultores de resposta a incidentes e fornecedores de equipamentos. Terceiros podem apoiar os ativos de TI ou TO da <Instituição>, além das atividades operacionais. Essas informações devem ser mantidas em um formato disponível para aqueles responsáveis pela gestão de riscos de terceiros.

E10-TERCEIROS-01-B

Terceiros que têm acesso, controle ou custódia de quaisquer ativos de TI, TO ou informação importantes para a execução da <Instituição> são identificados

Detalhamento:

Crie e mantenha uma lista que forneça informações básicas identificando partes internas e externas importantes que têm acesso, controle ou custódia de quaisquer ativos de TI, TO ou informações. Para algumas terceiras, como TI corporativa, esses relacionamentos importantes podem ser totalmente internos.

E10-TERCEIROS-01-C

Um método definido é seguido para identificar riscos decorrentes de fornecedores e outros terceiros

Detalhamento:

Um método definido é planejado antecipadamente, claramente descrito, tornado definido e padronizado. Empregar um método definido para identificar riscos decorrentes de fornecedores e outros terceiros ajudará os processos de gestão de riscos da <Instituição> a produzir resultados consistentes e permitirá uma gestão melhor do risco de terceiros.

E10-TERCEIROS-01-D

Terceiros são priorizados de acordo com critérios estabelecidos (por exemplo, importância para a entrega da <Instituição>, impacto de um compromisso ou interrupção, capacidade de negociar requisitos de cibersegurança dentro dos contratos)

Detalhamento:

A priorização de terceiros estabelece um ou mais subconjuntos de entidades nas quais a <Instituição> deve concentrar suas atividades de cibersegurança devido a critérios definidos, como sua importância para a entrega da <Instituição> ou seu papel como fornecedor crítico. A priorização e os critérios devem garantir que o esquema de priorização e a lista de terceiros priorizados sejam adequados ao ambiente de risco e à tolerância da <Instituição>. A falha em priorizar terceiros pode levar à proteção inadequada de ativos importantes e à atenção e recursos desproporcionais dedicados a terceiros, com impacto potencial limitado na função.

E10-TERCEIROS-01-E

A priorização escalonada é atribuída a fornecedores e outros terceiros cujo comprometimento ou interrupção pode causar consequências significativas (por exemplo, fornecedores de fonte única, fornecedores com acesso privilegiado)

Detalhamento:

Ao estabelecer critérios de priorização, a <Instituição> deve considerar situações em que a dependência de terceiros possa ser um ponto único de falha ou a interrupção de um serviço terceirizado possa ter impacto significativo na prestação do serviço. Por exemplo, se a <Instituição> depende de uma única fonte para conectividade de rede de área ampla em um local crítico, isso seria uma dependência de alta prioridade, pois a interrupção desse fornecimento teria o potencial de causar consequências organizacionais significativas.

E10-TERCEIROS-01-F

A priorização de fornecedores e outros terceiros é atualizada periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

A <Instituição> deve revisar a priorização de terceiros para garantir que os terceiros que representam maior risco para a <Instituição> recebam atenção adequada. Essa reavaliação da prioridade de terceiros pode ser impulsionada por um prazo definido ou por gatilhos definidos, como a aquisição de um produto de um novo fornecedor ou informações de fontes abertas sobre a situação financeira de uma empresa.

E10-TERCEIROS-02

Gerenciar riscos de terceiros

E10-TERCEIROS-02-A

A seleção de fornecedores e outros terceiros inclui a consideração de suas qualificações em cibersegurança

Detalhamento:

As qualificações de cibersegurança para fornecedores e outros terceiros podem incluir, por exemplo, manutenção de um nível especificado de implementação de controle de cibersegurança, incidentes cibernéticos anteriores envolvendo terceiros, verificações de antecedentes para pessoal que tem acesso a ativos críticos e requisitos para relatar violações e outros incidentes de cibersegurança.

E10-TERCEIROS-02-B

A seleção de produtos e serviços inclui a consideração de suas capacidades de cibersegurança

Detalhamento:

Os requisitos de cibersegurança para produtos e serviços podem incluir, por exemplo, a capacidade de desativar certas funcionalidades de um produto, uma compreensão clara dos componentes usados no produto e termos de serviço para um serviço que atendam aos requisitos de cibersegurança.

E10-TERCEIROS-02-C

Um método definido é seguido para identificar requisitos de cibersegurança e implementar controles associados que protejam contra riscos decorrentes de fornecedores e outros terceiros

Detalhamento:

Os requisitos de cibersegurança devem ser identificados de acordo com uma metodologia definida, eficaz e clara. Os requisitos devem incluir os controles necessários para proteger os produtos e serviços para enfrentar riscos de cibersegurança decorrentes de fornecedores e outras entidades identificadas

no <Eixo> RISCO. Consideração adicional deve ser dada a terceiros considerados pela <Instituição> como alta prioridade porque eles fornecem, mantêm ou operam componentes críticos de software essenciais para a operação da <Instituição>. A definição de um componente crítico de software pode variar amplamente dependendo da indústria ou do setor de infraestrutura crítica e pode ser informada por frameworks ou conjuntos de controle comumente utilizados. Por exemplo, o NIST fornece uma definição de software crítico sob a Ordem Executiva 14028 que alguma <Instituição> podem ser obrigadas a adotar

Controles de cibersegurança devem ser implementados para reduzir o risco que pode decorrer de fornecedores e outros terceiros. a <Instituição> pode implementar controles operacionais que restrinjam indivíduos de terceiros, como serviços de manutenção ou limpeza, de acessarem áreas projetadas da instalação sem escolta. Controles técnicos podem ser necessários para terceiros que fornecem um serviço como a manutenção remota de um ativo. a <Instituição> também pode considerar controles de gestão, como estratégias de aquisições que obscurecem o uso final de um ativo.

A seguir, estão exemplos dos tipos de requisitos a considerar:

• Controles e procedimentos para conceder acesso a terceiros

• Especificações para governança, proteção e destruição de dados

• Se o fornecedor irá desenvolver software e, em caso afirmativo, quais <Ações> de codificação segura devem ser utilizadas

• O conhecimento e habilidades necessários para desempenhar as responsabilidades atribuídas a terceiros

• Treinamento em cibersegurança que pode ser necessário antes de conceder acesso a terceiros

• Registro de dados, Retenção de registros e monitoramento

• Notificação, mitigação e coordenação de respostas de incidentes e vulnerabilidades, incluindo cronogramas e limites

• Resposta a incidentes e compartilhamento de informações

• Controles que regem conexões aos sistemas da <Instituição> por terceiros

• Se uma diversidade de softwares, ativos e fornecedores é necessária para reduzir o risco de exploração ampla de vulnerabilidades específicas

Fontes de informação para o desenvolvimento de requisitos de cibersegurança para fornecedores incluem análise de eventos cibernéticos anteriores (internos, externos e "quase acidentes"), brainstorming com partes interessadas internas, entrevistas com especialistas em cibersegurança, alertas de ameaças do setor, anúncios de vulnerabilidades, resultados de revisões internas de controle, avaliações de vulnerabilidades, testes de penetração e outras pesquisas.

E10-TERCEIROS-02-D

Um método definido é seguido para avaliar e selecionar fornecedores e outros terceiros

Detalhamento:

Usar um método definido para avaliação e seleção de terceiros ajuda a tornar esse processo consistente e repetível. Por exemplo, uma parte do método definido poderia descrever como a <Instituição> irá revisar as respostas dos fornecedores a pedidos de propostas (RFPs) para determinar se o fornecedor atende aos requisitos necessários. Isso pode incluir consideração de qualificações em cibersegurança, situação legal, bem-estar financeiro e relacionamentos com governos estrangeiros. As fontes de

informação podem incluir atestados fornecidos por terceiros (por exemplo, atestação da adequação e eficácia do ambiente de controle de cibersegurança) e verificações baseadas em histórico, informações de serviços de avaliação de terceiros e informações de fonte aberta.

E10-TERCEIROS-02-E

Requisitos de cibersegurança (por exemplo, notificação de vulnerabilidades, requisitos de SLA relacionados a incidentes) são formalizados em acordos com fornecedores e outros terceiros

Detalhamento:

Exigências na forma de especificações contratuais fornecem a base para acordos formais estabelecidos para definir e governar as relações entre a <Instituição> e as ações de entidades externas, incluindo mudanças relacionadas a produtos ou serviços entregues. Para cada acordo de terceiros, a <Instituição> deve estabelecer um conjunto detalhado de especificações que a terceira parte deve cumprir. Esses devem incluir os requisitos de cibersegurança que a <Instituição> espera que a terceira parte cumpra. É importante que essas especificações sejam completas, detalhadas, definitivas, adequadas para uso como critério na seleção de entidades externas, adequadas como linguagem em acordos com entidades externas e apropriadas para uso como base para monitorar o desempenho do terceiro. Idealmente, a equipe jurídica e técnica trabalhará em estreita colaboração no desenvolvimento desses requisitos. Por exemplo, a equipe técnica pode enfrentar desafios em relação à gestão de configuração quando há responsabilidade compartilhada pela operação dos ativos. a <Instituição> pode considerar o uso da linguagem contratual para garantir que a responsabilidade seja devidamente atribuída para resolver questões de configuração.

A linguagem do acordo pode ser usada para especificar expectativas e requisitos para notificação de vulnerabilidades ou incidentes, incluindo prazos, se a notificação é necessária antes da divulgação pública e mecanismos de comunicação a serem utilizados. Tais especificações são frequentemente documentadas em acordos de nível de serviço (SLAs) que são incluídos em pedidos de propostas (RFPs).

A redação do acordo deve definir o que constitui um evento, incidente e vulnerabilidade relacionados à entrega do produto ou serviço. Por exemplo, uma queda de serviço em uma região do país que pode afetar outras regiões pode ser um evento que o provedor de serviço deve informar à <Instituição>.

E10-TERCEIROS-02-F

Fornecedores e outros terceiros periodicamente atestan sua capacidade de atender aos requisitos de cibersegurança

Detalhamento:

Acordos com fornecedores e outros terceiros devem exigir atestação de que eles atendem aos requisitos de cibersegurança detalhados nos termos do acordo. Fornecedores e terceiros devem inicialmente atestar o cumprimento desses requisitos antes da assinatura do acordo, além de comprovar periodicamente que ainda cumprem os requisitos de cibersegurança. Para fornecedores-chave, validação adicional dos atestados pode ser considerada. Isso pode ser realizado por meio do monitoramento de incidentes relevantes, informações de serviços de avaliação terceirizados e informações de fonte aberta.

E10-TERCEIROS-02-G

Os requisitos de cibersegurança para fornecedores e outros terceiros incluem software seguro e requisitos de desenvolvimento de produtos seguros quando apropriado

Detalhamento:

A <Instituição> deve ter um processo padrão para definir requisitos seguros de desenvolvimento de software e produtos para terceiros. Para fornecedores que irão desenvolver software, por exemplo, determine e especifique quais <Ações> seguras de design e codificação são aceitáveis, como o NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM) e Open Web Application Security Project (OWASP). Requisitos de desenvolvimento seguro de produtos podem proibir o uso de componentes específicos com problemas conhecidos de cibersegurança.

Consideração adicional deve ser dada a terceiros considerados pela <Instituição> como alta prioridade (TERCEIROS-1c) porque eles fornecem, mantêm ou operam componentes críticos de software essenciais para a operação da <Instituição>. A definição de um componente crítico de software pode variar amplamente dependendo da indústria ou do setor de infraestrutura crítica e pode ser informada por frameworks ou conjuntos de controle comumente utilizados. Por exemplo, o NIST fornece uma definição de software crítico sob a Ordem Executiva 14028 que alguma <Instituição> podem ser obrigadas a adotar.

esta <Ação> está relacionada às atividades de arquitetura de cibersegurança associadas à seleção de fornecedores com base em suas <Ações> seguras de desenvolvimento de software (ARQUITETURA-4b e ARQUITETURA-4e).

E10-TERCEIROS-02-H

Os critérios de seleção para produtos incluem considerar prazos de fim e fim de vida útil

Detalhamento:

Terceiros devem ser selecionados de acordo com um processo organizado e minucioso, de acordo com especificações explícitas e critérios de seleção. O processo e os critérios de seleção devem ser elaborados para garantir que a entidade selecionada possa atender integralmente às especificações da <Instituição> conforme estabelecido. Esses critérios devem incluir a vida útil esperada do produto e os períodos de suporte ao produto.

E10-TERCEIROS-02-I

Os critérios de seleção incluem a consideração de salvaguardas contra software, hardware e serviços falsificados ou comprometidos

Detalhamento:

Terceiros devem ser selecionados de acordo com um processo organizado e minucioso, de acordo com especificações explícitas e critérios de seleção. O processo e os critérios de seleção devem ser elaborados para garantir que a entidade selecionada possa atender integralmente às especificações da <Instituição> conforme estabelecido.

Esses critérios devem incluir salvaguardas contra softwares, hardwares e serviços falsificados ou comprometidos. Por exemplo:

• O fornecedor divulgará a existência de todos os métodos conhecidos para burlar a autenticação de computador no produto adquirido, frequentemente chamados de backdoors, e fornecerá documentação

escrita de que todos esses backdoors criados pelo fornecedor foram permanentemente excluídos do sistema?

• O fornecedor fornecerá documentação resumida dos recursos de segurança do produto adquirido e instruções focadas em segurança sobre manutenção, suporte e reconfiguração das configurações padrão?

Para mais exemplos de critérios de aquisição de fornecedores que podem ser derivados da linguagem de compras, consulte a Linguagem de Compras de Cibersegurança do DOE para Sistemas de Entrega de Energia.

E10-TERCEIROS-02-J

Critérios de seleção para ativos de prioridade mais alta incluem a avaliação de listas de materiais para elementos-chave do ativo, como hardware e software

Detalhamento:

A criação, fabricação e montagem de ativos fornecidos por terceiros frequentemente compreendem muitos subcomponentes e subcomponentes provenientes de outros fornecedores e fornecedores. Uma <Instituição> que adquira esses ativos de terceiros podem, sem saber, herdar riscos cibernéticos que não foram identificados ou mitigados.

Uma lista de materiais estabelece e detalha a origem das subpartes e subcomponentes dos ativos adquiridos, incluindo sua origem e quaisquer informações adicionais que possam ajudar a <Instituição> a determinar o risco herdado. Exemplos desses subcomponentes e subcomponentes podem ser a incorporação de rotinas de software de bibliotecas de código aberto como componente de um build de software ou a obtenção de peças em uma câmera de segurança de um Estado-nação conhecido como hostil.

E10-TERCEIROS-02-K

Critérios de seleção para ativos de prioridade mais alta incluem avaliação de quaisquer ambientes de hospedagem de terceiros associados e dados de origem

Detalhamento:

Terceiros devem ser selecionados de acordo com um processo organizado e minucioso, de acordo com especificações explícitas e critérios de seleção. O processo e os critérios de seleção devem ser elaborados para garantir que a entidade selecionada possa atender integralmente às especificações da <Instituição> conforme estabelecido.

Para ativos de prioridade mais alta, esses critérios devem incluir a avaliação dos ambientes de hospedagem de terceiros associados e dos dados de origem.

Ambientes de hospedagem e dados fonte podem ser fontes significativas de risco adquirido. Ambientes de hospedagem compreendem muitas camadas de produtos e serviços que nem sempre estão sob o controle direto dos provedores de hospedagem e podem representar riscos não identificados para a <Instituição>. Por exemplo, podem incluir pacotes de software, bibliotecas de código aberto, configurações e outras configurações que foram usadas para construir uma máquina virtual que pode ser implantada em um ambiente de nuvem. Semelhante a uma lista de materiais, os ambientes de hospedagem devem fornecer documentação do uso desses produtos e serviços para que uma aproximação do risco adquirido possa ser estabelecida.

Além disso, esse conceito pode se estender à forma como A <Instituição> hospedadoras armazenam, processam e transmitem dados organizacionais. Avaliar os locais de armazenamento dos dados, onde são processados, como são transmitidos e os controles empregados é essencial para identificar riscos potenciais à confidencialidade, integridade e disponibilidade desses dados.

E10-TERCEIROS-02-L

O teste de aceitação dos ativos adquiridos inclui a consideração dos requisitos de cibersegurança

Detalhamento:

Quando o terceiro é responsável por produzir ou entregar ativos à <Instituição>, o processo de monitoramento deve incluir inspeção/teste dos ativos para garantir que atendam a todas as especificações declaradas, incluindo os requisitos de cibersegurança.

Por exemplo, se houver exigência de remover todos os componentes de software que não sejam necessários para a operação e/ou manutenção do produto adquirido (jogos, código-fonte, drivers não utilizados), ao receber o produto pode ser testado para a inclusão desses componentes.

E10-TERCEIROS-02-M

Controles de cibersegurança mais rigorosos são implementados para fornecedores de prioridade mais alta e outros terceiros

Detalhamento:

Nem todos os fornecedores expõem uma <Instituição> ao mesmo nível de risco. Como impor contratualmente requisitos específicos de cibersegurança pode resultar em custos aumentados, deve-se considerar garantir que os requisitos de cibersegurança sejam proporcionais ao risco potencial. Consideração adicional deve ser dada aos fornecedores de alta prioridade porque eles fornecem, mantêm ou operam componentes críticos de software essenciais para a operação da <Instituição>. A definição de um componente crítico de software pode variar amplamente dependendo da indústria ou do setor de infraestrutura crítica e pode ser informada por frameworks ou conjuntos de controle comumente utilizados. Por exemplo, o NIST fornece uma definição de software crítico sob a Ordem Executiva 14028 que alguma <Instituição> podem ser obrigadas a adotar. a <Instituição> deve implementar controles de cibersegurança mais rigorosos se for determinado que o impacto financeiro de um risco potencial será maior do que o custo calculado do risco.

E11-SITUAÇÃO

Consciência Situacional

Resumo:

A consciência situacional envolve o desenvolvimento de conhecimento quase em tempo real de um ambiente operacional dinâmico. Em parte, isso é feito por meio do registro e monitoramento de ativos de infraestrutura de TI, TO e comunicação essenciais para a entrega da função. É igualmente importante manter o conhecimento dos eventos relevantes e atuais de cibersegurança externos à <Instituição>. Uma vez que uma <Instituição> desenvolve consciência situacional, ela pode alinhar estados predefinidos de operação às mudanças no ambiente operacional. A capacidade de mudar de um estado predefinido para outro pode permitir uma resposta mais rápida e eficaz a eventos de cibersegurança ou mudanças no ambiente de ameaças.

Detalhamento:

Registros de logs devem ser habilitados com base no impacto potencial de um ativo na função. Por exemplo, quanto maior o impacto potencial de um ativo comprometido, mais dados uma <Instituição> pode coletar sobre o ativo.

O monitoramento e a análise dos logs e outros dados coletados permitem que a <Instituição> compreenda o status operacional e de cibersegurança da função. Comunicar efetivamente o status operacional, de segurança e de ameaças aos tomadores de decisão relevantes é a essência da consciência situacional (às vezes chamada de visão operacional comum). Embora muitas implementações de consciência situacional possam incluir ferramentas de visualização, como painéis, mapas e outras representações gráficas, elas não são necessariamente obrigatórias para atingir o objetivo.

E11-SITUAÇÃO-01

Executar registro

E11-SITUAÇÃO-01-A

O registro ocorre para ativos que são importantes para a entrega da <Instituição>

Detalhamento:

Ative o registro de ativos importantes. Algumas atividades que podem ser registradas incluem as ações de pessoas, objetos e entidades ao acessarem e usar ativos, eventos que podem interromper a entrega da <Instituição>, alterações em ativos que fogem da configuração básica, ativos inesperados conectando-se a redes e qualquer atividade inesperada ou suspeita. Isso também pode incluir ativos virtualizados desligados involuntariamente, deletados ou "esgotados de recursos".

E11-SITUAÇÃO-01-B

O registro de registros ocorre para ativos dentro da <Instituição> que podem ser aproveitados para atingir um objetivo de ameaça, sempre que possível

Detalhamento:

Esta <Ação> se baseia nas atividades de registro identificadas para incluir ativos que podem ser usados na busca dos objetivos dos agentes ameaçadores. Um ator ameaçador pode usar múltiplas táticas, como as definidas no Marco MITRE ATT&CK, para alcançar seu objetivo final de ameaça (por exemplo, extorsão, manipulação de dados, roubo de propriedade intelectual, roubo de dados de clientes,

sabotagem). A exploração pode não ser viável para todos os tipos de ativos dentro da <Instituição>. Quando o registro não é viável, a <Instituição> podem considerar implementar controles de mitigação, como limitar o acesso físico ou lógico.

E11-SITUAÇÃO-01-C

Requisitos de registro são estabelecidos e mantidos para ativos de TI que são importantes para a entrega da <Instituição> e ativos dentro da <Instituição> que podem ser aproveitados para alcançar um objetivo de ameaça

Detalhamento:

Defina os requisitos de registro para todos os ativos importantes de TI. Por exemplo, capturar tentativas de login falhadas pode indicar problemas de confidencialidade, alterações não autorizadas podem indicar problemas de integridade, e entradas de log em períodos de inatividade do sistema podem revelar problemas de disponibilidade. Os requisitos para registro podem variar para diferentes ativos, como tecnologia operacional, dispositivos de campo, dispositivos móveis e ativos que residem na nuvem. Para redes virtuais, ferramentas ou processos adicionais podem ser necessários para permitir o registro do tráfego de rede virtual. Logs da nuvem, incluindo tanto infraestrutura quanto ativos em nuvem, devem ser definidos pela <Instituição> nos requisitos de registro conforme aplicável. Além dos tipos de eventos a serem registrados, a <Instituição> deve considerar quais requisitos de registro podem ser apropriados, como como os registros devem ser protegidos, considerações sobre a cadeia de custódia ou prazos de retenção.

Exemplos de eventos que podem ser registrados:

1. Eventos de administração do sistema operacional e aplicação

• Criação e exclusão de contas

• Atribuição de privilégios de contas

• Alterações de configuração ou instalação de software

2. Eventos de uso do sistema operacional e da aplicação

• Inicialização, desligamento e falha de serviços e aplicações

• Conexões e falhas na rede

• Tentativas bem-sucedidas e não bem-sucedidas de login

• Falhas na aplicação

• Tráfego de e-mail e web

• Sistemas e arquivos acessados pelos usuários

3. Eventos ocorrendo em dispositivos de rede como

• Firewalls

• Switches

• Roteadores

• Pontos de acesso sem fio

4. Eventos ocorrendo em dispositivos TO como

• Interfaces homem-máquina (HMIs) e estações de trabalho de operadores

• Relés de proteção

• Controladores lógicos programáveis (PLCs)

• Unidades terminais remotas (RTUs)

• Medidores inteligentes

E11-SITUAÇÃO-01-D

Os requisitos de registro são estabelecidos e mantidos para infraestrutura de monitoramento de rede e host (por exemplo, gateways web, software de detecção e resposta de endpoints, sistemas de detecção e prevenção de intrusões)

Detalhamento:

Defina os requisitos de registro para toda a infraestrutura de monitoramento de rede e host. Esses requisitos podem ser diferentes de outros ativos de TI, pois podem fornecer informações adicionais que podem ser úteis para construir uma compreensão completa das atividades dentro das redes da <Instituição>. Por exemplo, logs de eventos de um portal web que mostram conexões para sites bloqueados porque violaram a política da empresa.

E11-SITUAÇÃO-01-E

Os dados de log estão sendo agregados dentro da <Instituição>

Detalhamento:

Colete dados de log de diferentes ativos e agregue em um repositório central. A agregação pode ser realizada dentro da <Instituição> ou em outra parte da empresa, dependendo de várias considerações, como arquitetura empresarial e requisitos regulatórios. O repositório pode ser um simples servidor de logs, ou infraestrutura de gerenciamento de logs que inclui servidores de log centralizados e armazenamento de dados de log, ou um sistema de gerenciamento de informações e eventos de segurança (SIEM) suportado por fornecedores. Fazer isso torna os dados de log disponíveis mesmo quando ativos individuais estão offline ou destruídos. A agregação pode ser especialmente benéfica para coletar informações de ativos de tecnologia operacional com capacidade limitada de registro local.

Além disso, ao agregar dados de log de vários ativos, a <Instituição> pode correlacionar dados para identificar padrões e anomalias.

E11-SITUAÇÃO-01-F

Registros mais rigorosos são realizados para ativos de prioridade mais alta

Detalhamento:

Os requisitos de registro são aprimorados para incluir a consideração de riscos em nível de ativos identificados por meio das atividades de gestão de riscos, de modo que um registro mais rigoroso seja realizado para ativos de maior risco. No contexto desta <Ação>, mais rigoroso descreve uma abordagem de registro que é completa e abrangente, inclui a cobertura de todos os controles chave, é regularmente revisada e ajustada com base em mudanças ambientais, e é persistente e contínua (em vez de intermitente e discreta).

Por exemplo, para o gerenciamento de ativos virtualizados, a <Instituição> pode exigir que informações adicionais de log sejam capturadas, como ID do usuário, carimbos de data e o endereço IP do terminal do usuário. Uma <Instituição> que possua capacidades de registro muito maduras, sem

oportunidade de implementação adicional desta <Ação> como escrita, deve considerar uma resposta de implementação total.

E11-SITUAÇÃO-02

Executar monitoramento

E11-SITUAÇÃO-02-A

Revisões periódicas de dados de log ou outras atividades de monitoramento de cibersegurança são realizadas

Detalhamento:

A revisão e auditoria regular dos registros de eventos (manualmente ou por ferramentas automatizadas) é uma atividade crítica de monitoramento essencial para a consciência situacional (por exemplo, por meio da detecção de eventos ou fraquezas de cibersegurança). Por exemplo, logs podem fornecer dados sobre mudanças no ambiente do usuário que podem resultar em mudanças necessárias nos privilégios de acesso ou acionar alertas quando sistemas importantes para a entrega da <Instituição> não estão disponíveis. Outro exemplo disso são ativos virtualizados desativados, excluídos ou "esgotados de recursos" sem querer, que podem disparar alertas para garantir que os administradores estejam cientes de atualizações ou patches do sistema que podem não ter sido aplicados a esses sistemas enquanto estavam offline ou incapazes de responder.

E11-SITUAÇÃO-02-B

Dados e alertas dos ativos de infraestrutura de monitoramento de rede e host são revisados periodicamente

Detalhamento:

Atividade anômala é aquela que é inconsistente ou que se desvia do que é usual, normal ou esperado. O monitoramento deve fornecer as informações necessárias para a <Instituição> determinar se está sendo submetida a um evento de cibersegurança que possa exigir ações para evitar impacto organizacional. Isso pode incluir, por exemplo, a revisão de dados de logs de rede para identificar conexões não autorizadas com ativos importantes para a entrega da <Instituição>. Isso também pode incluir observações feitas por pessoal da sala de controle e outros funcionários de operações sobre respostas inesperadas do sistema, leituras de sensores ou outras atividades inexplicadas exibidas pelos sistemas operacionais. Parte da intenção desta <Ação> é incluir as pessoas como parte da abordagem geral de uma <Instituição> para monitorar seus sistemas.

E11-SITUAÇÃO-02-C

Requisitos de monitoramento e análise são estabelecidos e mantidos para a <Instituição> e para a revisão oportuna dos dados de eventos

Detalhamento:

Requisitos de monitoramento e análise definem as atividades necessárias para fornecer informações às partes interessadas em toda a <Instituição> de forma regular, a fim de proteger e sustentar ativos de TI, TO e informação essenciais para a execução da <Instituição>. O desenvolvimento dos requisitos deve identificar os principais interessados e como os requisitos de monitoramento e análise satisfarão suas necessidades de informação. Os requisitos de monitoramento podem ser diferentes para ativos como tecnologia operacional, dispositivos de campo, dispositivos móveis, ativos virtualizados e ativos residentes na nuvem. Os requisitos devem descrever quais dados devem ser coletados e como devem

ser analisados. Os requisitos também devem especificar parâmetros de tempo para a revisão dos dados coletados e como esses dados serão distribuídos.

Os requisitos devem considerar:

• Tipo de dados e extensão dos dados necessários

• A granularidade dos dados necessários.

• O formato dos dados

• A frequência de distribuição dos dados

• Como os dados serão distribuídos

• O prazo de retenção dos dados

• Com que frequência as revisões devem ser realizadas

E11-SITUAÇÃO-02-D

Indicadores de atividade anômala são estabelecidos e mantidos com base em logs do sistema, fluxos de dados, linhas de base de rede, eventos de cibersegurança e arquitetura, sendo monitorados em ambientes de TI

Detalhamento:

A <Instituição> deve definir e monitorar indicadores de atividade anômala que sejam relevantes para suas operações. Indicadores são sinais de que um incidente pode ter ocorrido ou pode estar ocorrendo agora. Isso pode incluir tentativas de login falhadas, novas conexões de dispositivos, varredura de portas, transferências de arquivos em grande volume e variações de disponibilidade para um sistema. Os indicadores podem não ser necessariamente maliciosos, mas fogem da norma e exigem monitoramento adicional.

Indicadores de atividade anômala também podem ser identificados por meio da análise de eventos de cibersegurança "quase acidentes". Esses eventos podem incluir eventos internos da sua <Instituição> ou aqueles que ocorrem externamente em outra <Instituição>. Os indicadores podem não ser necessariamente maliciosos, mas fogem da norma e exigem monitoramento adicional.

E11-SITUAÇÃO-02-E

Alarmes e alertas são configurados e mantidos para apoiar a identificação de eventos de cibersegurança

Detalhamento:

Os requisitos de monitoramento devem incluir especificações para alarmes e alertas para auxiliar na identificação de eventos de cibersegurança, como limiares, durações e fontes de atividade. Por exemplo, um alarme pode ser configurado para ser acionado quando as requisições de conexão excedem um número específico que é o máximo estabelecido para atividade normal, indicando assim a possibilidade de um ataque de negação de serviço.

E11-SITUAÇÃO-02-F

As atividades de monitoramento estão alinhadas com o perfil de ameaça (AMEAÇA-2e)

Detalhamento:

Os requisitos de monitoramento devem incluir (entre outras coisas) atividades que coletem informações relevantes para o perfil de ameaça da <Instituição>. Para alinhar o monitoramento ao perfil de ameaça, a <Instituição> deve revisar os ativos-alvo, objetivos e métodos de ataque que podem ser empregados pelos agentes ameaçadores e ajustar as atividades de monitoramento de acordo. Por exemplo, se o perfil de ameaça incluir uma ameaça envolvendo um ator de Estado-nação conhecido por usar spear phishing, o e-mail pode ser monitorado para características específicas conhecidas nesses e-mails de phishing.

E11-SITUAÇÃO-02-G

Monitoramento mais rigoroso é realizado para ativos de prioridade mais alta

Detalhamento:

Os requisitos de monitoramento são aprimorados para incluir a consideração dos riscos em nível de ativos identificados por meio das atividades de gestão de riscos, de modo que um monitoramento mais rigoroso seja realizado para ativos de maior risco (como ativos considerados importantes para a execução da <Instituição>, sistemas de segurança e ativos contendo informações sensíveis). No contexto desta <Ação>, mais rigoroso descreve uma abordagem completa e abrangente, que inclui a cobertura de todos os controles chave, que é regularmente revisada e ajustada com base em mudanças ambientais, e que é persistente e contínua (em vez de intermitente e discreta).

Por exemplo, a <Instituição> pode estabelecer requisitos para monitorar registros de acesso para ativos contendo dados sensíveis. Uma <Instituição> que possua capacidades de monitoramento muito maduras, sem oportunidade de implementação adicional desta <Ação> como escrita, devem considerar uma resposta de implementação total.

E11-SITUAÇÃO-02-H

A informação de análise de risco (RISCO-3d) é usada para identificar indicadores de atividade anômala

Detalhamento:

Atividades de registro e requisitos de monitoramento e análise são aprimorados para incorporar informações relevantes das atividades de análise de risco. A equipe de monitoramento revisa regularmente as informações da análise de risco e modifica indicadores existentes de atividade anômala ou desenvolve outros adicionais com base em atualizações sobre ameaças, vulnerabilidades e riscos identificados.

E11-SITUAÇÃO-02-I

Indicadores de atividade anômala são avaliados e atualizados periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

Indicadores de atividade anômala são revisados quanto à eficácia e atualizados conforme necessário pela equipe de monitoramento para garantir que ainda estejam atendendo aos requisitos definidos de monitoramento e às necessidades de informações das partes interessadas. A revisão e atualização devem ser realizadas com uma frequência definida pela <Instituição> que garanta que os indicadores estejam atualizados com base nas informações de risco da <Instituição>.

Por exemplo, uma <Instituição> pode monitorar fontes públicas disponíveis (por exemplo, Banco de Dados Nacional de Vulnerabilidades (NVD), CISA Central e CERT/CC) para obter informações sobre novas vulnerabilidades e exploits e identificar novos indicadores potenciais de atividade anômala.

E11-SITUAÇÃO-03

Estabelecer e manter a consciência situacional

E11-SITUAÇÃO-03-A

Métodos de comunicação sobre o estado atual da cibersegurança para a <Instituição> são estabelecidos e mantidos

Detalhamento:

Métodos para comunicar efetivamente o estado atual da cibersegurança aos tomadores de decisão relevantes podem incluir mecanismos (como quadros de avisos, painéis eletrônicos de tela grande, árvores de chamadas e telefones via satélite) e uma linguagem comum e termos definidos para descrever informações de cibersegurança (como níveis de ameaça). Essas devem ser avaliadas e atualizadas regularmente conforme necessário para garantir que continuem sendo eficazes na expressão de todas as condições de cibersegurança.

E11-SITUAÇÃO-03-B

Os dados de monitoramento são agregados para fornecer uma compreensão do estado operacional da <Instituição>

Detalhamento:

A agregação de dados de monitoramento pode ser usada para determinar se a <Instituição> está operando como esperado, incluindo acesso a recursos de rede compartilhados, largura de banda e controles de acesso ao sistema. O valor dessa coleta de dados é ampliado pela criação de métricas operacionais minimamente aceitáveis e alvo para componentes críticos do sistema, permitindo a identificação imediata de situações subótimas e a possível degradação da <Instituição>. Os dados de monitoramento a serem agregados podem vir de várias fontes, incluindo aquelas fora da <Instituição> em escopo da autoavaliação.

E11-SITUAÇÃO-03-C

Informações relevantes de toda a <Instituição> estão disponíveis para aumentar a consciência situacional

Detalhamento:

Além dos dados coletados por meio do monitoramento, há processos em vigor para coletar informações relevantes que podem adicionar detalhes ou clareza à consciência situacional, ou ajudar a corroborar múltiplas fontes de informações semelhantes. Informações relevantes podem incluir relatórios pós-ação de incidentes, ligações para help desks sobre atividades suspeitas, além de relatórios e estatísticas sobre tentativas de phishing. A consciência situacional é mais completa quando utiliza múltiplas fontes de informação.

E11-SITUAÇÃO-03-D

Requisitos de relatórios de consciência situacional foram definidos e tratam da disseminação oportuna das informações de cibersegurança para as partes interessadas definidas pela <Instituição>

Detalhamento:

Os requisitos de relatórios de consciência situacional devem definir o desenvolvimento, a entrega e a manutenção das comunicações de consciência situacional necessárias para cada tipo de parte interessada. Por exemplo, comunicações de consciência situacional para as autoridades diferirão significativamente das que se comunicam ao conselho de administração. O plano deve abordar o desenvolvimento e a execução de curto prazo e deve ser ajustado com certa regularidade em resposta a novas ou mudanças de necessidades e a partir da avaliação da eficácia das atividades de comunicação.

Estes são exemplos de partes interessadas para relatórios de conscientização situacional:

• Líderes organizacionais

• Liderança e membros da equipe do programa de cibersegurança

• Indivíduos em toda a <Instituição> para quem um incidente de cibersegurança teria impacto

• Centros de compartilhamento e análise

de informações

• Entidades governamentais

• Forças de segurança

• Organizações conectadas

• Fornecedores

• Associações setoriais (a exemplo de associações comerciais)

• Reguladores

Estes são exemplos de requisitos de relatórios de consciência situacional:

• A frequência e o momento das comunicações

• Controles especiais sobre comunicações (por exemplo, criptografia ou comunicações seguras) que são apropriados para algumas partes interessadas

• Recursos necessários

• Recursos internos e externos envolvidos no suporte ao processo de comunicação

• Pontos de contato internos e externos por função

• Métodos e canais de comunicação a serem utilizados

• Os ativos, pessoas e sistemas (incluindo sistemas externos como redes celulares) que podem estar indisponíveis durante a resposta e quais recursos de backup podem ser necessários

E11-SITUAÇÃO-03-E

Informações relevantes de fora da <Instituição> são coletadas e disponibilizadas em toda a <Instituição> para aumentar a consciência situacional

Detalhamento:

Além dos dados coletados por meio de monitoramento e fontes internas de informação, existem processos para coletar informações de uma <Instituição> externa que pode agregar detalhes ou clareza à consciência situacional. Por exemplo, a equipe pode monitorar e coletar informações de diversos recursos que fornecem informações confiáveis de cibersegurança, como fóruns, fornecedores, InfraGard, ISACs e CISA Central. Dados externos são analisados antes do compartilhamento para

garantir que as informações compartilhadas sejam relevantes e úteis para os destinatários e para destacar áreas específicas de atenção. As informações de consciência situacional são então compartilhadas com partes interessadas apropriadas, como liderança organizacional, pessoal de resposta a incidentes e proprietários de ativos.

E11-SITUAÇÃO-03-F

É estabelecida e mantida uma capacidade para agregar, correlacionar e analisar os resultados das atividades de monitoramento de cibersegurança e fornecer uma compreensão quase em tempo real do estado de cibersegurança da <Instituição>

Detalhamento:

A agregação de dados de monitoramento normalmente envolve o uso de ferramentas avançadas de monitoramento, como sistemas de gerenciamento de informações e eventos de segurança (SIEM), para agregar logs do sistema e dados de rede, permitindo uma análise mais holística do ambiente. Embora não seja um requisito para a implementação desta <Ação>, a <Instituição> pode considerar a agregação de dados de monitoramento de várias funções. Semelhante à agregação dentro de uma função, o compartilhamento e análise dos dados de monitoramento entre as funções da <Instituição> proporciona uma consciência mais abrangente do estado operacional e da cibersegurança da <Instituição>. Isso pode exigir a implementação de métodos para resumir ou simplificar as informações apresentadas àqueles que revisam logs agregados de auditoria (por exemplo, redução de relatórios).

E11-SITUAÇÃO-03-G

Estados de operação predefinidos são documentados e podem ser implementados com base no estado de cibersegurança da <Instituição> ou quando acionados por atividades em outros <Eixos>

Detalhamento:

Estados de operação predefinidos são modos operacionais distintos (que normalmente incluem configurações específicas de TI, bem como procedimentos alternativos ou modificados) que foram projetados e implementados para a <Instituição> e podem ser invocados por um processo manual ou automatizado em resposta a um evento, um ambiente de risco em mudança ou outros dados sensoriais e de conscientização para proporcionar maior segurança, resiliência, confiabilidade e/ou cibersegurança.

Definir estados de operação predefinidos normalmente requer o uso de arquiteturas ou topologias detalhadas, documentação e compreensão detalhada dos seus ativos e suas prioridades, categorias e atributos.

Os estados definidos podem incluir critérios para invocar o estado, como quem tem autoridade para acionar uma mudança de estado em qualquer direção, listas de verificação que devem ser preenchidas antes de passar de um estado degradado para um estado operacional, quanto tempo a <Instituição> pode sobreviver em um determinado estado ou como ela realizará o monitoramento para determinar quando os critérios são atendidos. Informações das atividades de monitoramento são usadas para acionar decisões sobre a invocação dos estados de operação predefinidos.

Por exemplo, se as atividades de monitoramento indicarem uma interrupção, isso pode desencadear um processo manual no qual uma análise é feita determinando que nem todas as operações podem ser suportadas, determinadores específicos devem aprovar a restrição temporária de operações não essenciais, e um estado pré-definido é invocado no qual certos ativos são desligados.

Outras situações podem usar um processo automatizado. Por exemplo, com base em inteligência de ameaças recebida por meio de atividades de monitoramento, um conjunto de regras aciona uma atualização do nível de ameaça, que aciona a invocação de um estado pré-definido que desliga ativos críticos. Outro exemplo de estados predefinidos de operação pode ser limitar as comunicações entre ambientes de TI durante um incidente de cibersegurança.

Como outro exemplo, situações de alto-risco podem ser identificadas que justificam registro adicional, como uma emergência relacionada à segurança que exige uma elevação imediata dos privilégios de acesso, mas também podem aumentar a verbosidade do loging nos dispositivos afetados.

E12-ARQUITETURA

Arquitetura de cibersegurança

Resumo:

Estabelecer uma arquitetura de cibersegurança envolve identificar os requisitos de cibersegurança para os ativos da <Instituição> e projetar controles apropriados para protegê-los. A arquitetura de cibersegurança serve como referência para orientar como a cibersegurança deve ser implementada para atender aos objetivos da estratégia do programa de cibersegurança.

Detalhamento:

O <Eixo> de Arquitetura de Cibersegurança é focado na <Instituição>. As <Ações> descritas em <Eixos> focados na <Instituição> são frequentemente realizadas como parte de um programa corporativo e podem ser estabelecidas e operar independentemente da função em questão. Para levar isso em consideração, o objetivo inicial em cada <Eixo> focado na <Instituição> concentra-se no estabelecimento e na manutenção do programa relacionado.

A arquitetura de cibersegurança ajuda uma <Instituição> a planejar a maneira como a segurança deve ser projetada de maneira holística e integrada. Facilita uma abordagem proativa e fundamentada para planejar futuras melhorias de segurança para ativos, sistemas e a <Instituição> como um todo. Os controles de arquitetura podem se concentrar em vários recursos importantes de cibersegurança para uma <Instituição>, como detectar, resistir, reagir e se recuperar de ciberataques. Essas táticas incluem segmentação, controles criptográficos, monitoramento e redundância. Além disso, como uma arquitetura de cibersegurança é uma ferramenta de planejamento voltada para o futuro, deve-se considerar não apenas as tendências tecnológicas atuais, mas também possíveis desenvolvimentos futuros, como a computação quântica e os riscos associados que ela pode representar para os sistemas de criptografia existentes. Para que a arquitetura de cibersegurança seja eficaz, os responsáveis por ela devem ser incluídos nos processos de planejamento e tomada de decisão quando mudanças na <Instituição>, sistemas de TI ou sistemas TO estiverem sendo consideradas. Dessa forma, as alterações na <Instituição> podem ser revisadas para resolver questões de segurança e garantir que o resultado esteja alinhado com a tolerância ao risco de cibersegurança da <Instituição>.

E12-ARQUITETURA-01

Estabelecer e manter a estratégia e o programa de arquitetura de cibersegurança

E12-ARQUITETURA-01-A

A <Instituição> possui uma estratégia para arquitetura de cibersegurança

Detalhamento:

Há um resultado desejado para a estratégia de arquitetura de cibersegurança e um consenso sobre como alcançá-lo. Por exemplo, a estratégia de arquitetura pode estar focada em prevenir acessos não autorizados, e há consenso sobre as decisões de design relativas às soluções propostas de autenticação e autorização.

E12-ARQUITETURA-01-B

Uma estratégia para a arquitetura de cibersegurança é estabelecida e mantida em alinhamento com a estratégia do programa de cibersegurança da <Instituição> e a arquitetura empresarial

Detalhamento:

A estratégia de arquitetura de cibersegurança é mantida atualizada e relevante. Uma estratégia de arquitetura de cibersegurança para proteger sistemas mainframe legados, por exemplo, provavelmente estará fora de sintonia com o objetivo de um programa de cibersegurança de acomodar dispositivos móveis seguros e com a meta da arquitetura empresarial de migrar para a nuvem e fornecer dados como um ativo em toda a empresa.

E12-ARQUITETURA-01-C

Uma arquitetura documentada de cibersegurança é estabelecida e mantida, incluindo sistemas e redes de TI, alinhando-se com a categorização e priorização de sistemas e ativos

Detalhamento:

A arquitetura de cibersegurança é documentada para que possa ser comunicada e revisada por partes interessadas importantes. A arquitetura de cibersegurança apoia o raciocínio sobre priorização de ativos e importantes salvaguardas arquitetônicas relacionadas às interações entre ativos de TI. Por exemplo, decisões de design sobre limites de confiança precisam ser documentadas em termos dos elementos arquitetônicos envolvidos e das trocas de informações entre eles. A arquitetura de cibersegurança deve incluir considerações apropriadas para ativos usados na entrega da <Instituição> ou que possam aumentar o risco cibernético para a <Instituição>, incluindo ativos móveis, equipamentos pessoais de computação e redes usados para conectividade remota, dispositivos de campo, VoIP, sistemas de sinalização e outros sistemas físicos de acesso, além de sinalização digital.

E12-ARQUITETURA-01-D

A governança para arquitetura de cibersegurança (como um processo de revisão de arquitetura) é estabelecida e mantida, incluindo disposições para revisões arquitetônicas periódicas e um processo de exceções

Detalhamento:

Há supervisão suficiente da arquitetura de cibersegurança ou da <Instituição> de governança equivalente da arquitetura de cibersegurança para evitar desvio arquitetônico — a discrepância entre a arquitetura documentada e a arquitetura implementada. Por exemplo, mudanças propostas na arquitetura estão sujeitas a revisão e aprovação, e exceções são aprovadas com conhecimento dos riscos e consequências.

E12-ARQUITETURA-01-E

O patrocínio da alta gestão para o programa de arquitetura de cibersegurança é visível e ativo

Detalhamento:

O patrocínio visível e ativo da alta administração pode incluir comunicações regulares da alta administração sobre a importância e o valor da arquitetura de cibersegurança, apoio organizacional para o estabelecimento e implementação da governança da arquitetura de cibersegurança (como um processo de revisão de arquitetura), e financiamento de prêmios e programas de reconhecimento para funcionários que contribuem significativamente para alcançar os objetivos de cibersegurança.

E12-ARQUITETURA-01-F

A arquitetura de cibersegurança estabelece e mantém os requisitos de cibersegurança para os ativos da <Instituição>

Detalhamento:

Selecione e documente os requisitos para o nível adequado de confidencialidade, integridade e disponibilidade de ativos de TI, TO e informações. Uma expressão comum desses requisitos são políticas organizacionais associadas à seleção e implementação de controles para os ativos da <Instituição>.

E12-ARQUITETURA-01-G

Os controles de cibersegurança são selecionados e implementados para atender aos requisitos de cibersegurança

Detalhamento:

A arquitetura de cibersegurança inclui decisões de design — táticas — para implementar requisitos de cibersegurança definidos no <Eixo> ARQUITETURA. Por exemplo, a confidencialidade — a exigência de não divulgar informações sensíveis a partes não autorizadas — pode ser realizada por meio de um controle que garante que nenhuma informação de cartão de crédito seja mantida por uma interface web após a conclusão da transação de pagamento. Como outro exemplo, confidencialidade e integridade podem ser abordadas colocando controles adicionais de criptografia em conexões externas, como celular, satélite ou fibra municipal fornecidas por uma entidade externa. Controles selecionados são documentados na arquitetura de cibersegurança.

E12-ARQUITETURA-01-H

A estratégia e o programa de arquitetura de cibersegurança estão alinhados com a estratégia e o programa de arquitetura empresarial da <Instituição>

Detalhamento:

O alinhamento dessas estratégias evita expectativas desalinhadas entre partes interessadas do negócio e técnicas. Por exemplo, os objetivos empresariais de proteger propriedade intelectual e dados empresariais sensíveis são apoiados pelos objetivos de cibersegurança de minimizar superfícies de ataque e estabelecer padrões seguros.

E12-ARQUITETURA-01-I

A conformidade dos sistemas e redes da <Instituição> com a arquitetura de cibersegurança é avaliada periodicamente e de acordo com gatilhos definidos, como mudanças no sistema e eventos externos

Detalhamento:

A arquitetura de cibersegurança é tratada como um recurso que ajuda a manter a postura de segurança da <Instituição>. Avaliações periódicas de conformidade com a arquitetura de cibersegurança são uma técnica de redução de risco. Por exemplo, uma proposta de reaproveitamento ou virtualização de um servidor é uma decisão de design que deve ser avaliada quanto ao seu efeito na arquitetura. As avaliações devem incluir dispositivos que possam aumentar o risco cibernético para a <Instituição>, como ativos móveis, equipamentos pessoais de computação e redes usados para conectividade remota, dispositivos de campo, VoIP, badges e outros sistemas de acesso físico, além de sinalização digital. Técnicas avançadas de cibersegurança, como caça a ameaças e defesa ativa, podem ajudar a identificar sistemas ou redes não conformes.

E12-ARQUITETURA-01-J

A arquitetura de cibersegurança é guiada pelas informações de análise de risco (RISCO-3d) e pelo perfil de ameaças (AMEAÇA-2e) da <Instituição>

Detalhamento:

Resultados de análise de risco, como categorias de risco priorizadas e informações de perfil de ameaça, como alvos em certos tipos de ataques, são fontes potenciais de informação sobre as táticas arquitetônicas prováveis necessárias para detectar, resistir, reagir e se recuperar de ataques em campo. Para alinhar a arquitetura de cibersegurança com o perfil de ameaça, a <Instituição> pode revisar os ativos-alvo, objetivos e métodos de ataque que podem ser empregados pelos atores ameaçadores e ajustar a arquitetura de cibersegurança de acordo. Por exemplo, manter uma trilha de auditoria é uma tática para apoiar a responsabilidade e a recuperação de ataques inimigos, e fornecer servidores redundantes é uma tática para apoiar a disponibilidade e a continuidade do negócio.

E12-ARQUITETURA-01-K

A arquitetura de cibersegurança aborda estados de operação predefinidos

Detalhamento:

O design da arquitetura de cibersegurança deve levar em conta os requisitos necessários para suportar estados de operação predefinidos que possam precisar ser engajados pela <Instituição>. Por exemplo, requisitos de monitoramento podem precisar ser incorporados à arquitetura para ajudar a apoiar decisões de desligamento dos ativos caso haja indicadores de uma possível interrupção. Como outro exemplo, se ocorrer um incidente relacionado à segurança e uma elevação temporária de privilégios for necessária, o sistema pode automaticamente aumentar a verbosidade do registro de dados.

E12-ARQUITETURA-02

Implementar proteções de rede como um elemento da arquitetura de cibersegurança

E12-ARQUITETURA-02-A

Proteções de rede são implementadas

Detalhamento:

Proteções são implementadas que atendem aos resultados desejados na estratégia de arquitetura de cibersegurança. No contexto do <Eixo> ARQUITETURA, a implementação dessas proteções baseia-se em requisitos padronizados documentados em uma arquitetura de cibersegurança. Como esta <Ação> pode ser realizada de forma ad hoc, elas podem, em geral, estar alinhadas a esses requisitos, mas podem não ser implementadas de acordo com um processo ou procedimento documentado.

E12-ARQUITETURA-02-B

Os sistemas de TI da <Instituição> são separados dos sistemas de TO por segmentação, seja por meios físicos ou lógicos

Detalhamento:

Essa é uma abordagem mínima, que vai desde firewalls até servidores de acesso remoto (também conhecidos como jump boxes). Segmentação é uma tática arquitetônica que fornece uma primeira linha de defesa voltada para conter a propagação de ataques e prevenir a travessia de agentes maliciosos entre sistemas (por exemplo, sistemas voltados para a Web, sistemas de TI e sistemas TO). A

segmentação pode incluir separação, implementação de zonas de confiança, implementação de zonas desmilitarizadas (DMZs) ou outras táticas arquitetônicas.

E12-ARQUITETURA-02-C

Proteções de rede são definidas e aplicadas para tipos selecionados de ativos de acordo com risco e prioridade do ativo (por exemplo, ativos internos, ativos perimetrais, ativos conectados ao Wi-Fi da <Instituição>, ativos em nuvem, acesso remoto e dispositivos de propriedade externa)

Detalhamento:

As proteções de rede devem ser projetadas para impor controles definidos com base em diferentes tipos de ativos. A decisão de implementar controles mais rigorosos pode ser baseada em fatores como a confiança em certos tipos de ativos ou a sensibilidade das informações acessadas por um tipo de ativo. Por exemplo, conexões remotas podem apresentar riscos maiores e estariam sujeitas a proteções adicionais. Alternativamente, ativos de TI que operam apenas na rede interna podem ser mais confiáveis e, portanto, exigir proteções de rede menos rigorosas.

E12-ARQUITETURA-02-D

Ativos importantes para a entrega da <Instituição> são segmentados logicamente ou fisicamente em zonas de segurança distintas, baseadas nos requisitos de cibersegurança dos ativos

Detalhamento:

Esta <Ação> expande a arquitetura para incluir ativos importantes para a entrega da <Instituição>. A <Ação> segue observando que a segmentação deve ser baseada em requisitos definidos de cibersegurança. Os critérios para a criação de diferentes zonas de segurança podem ser baseados em vários fatores. Estes são alguns exemplos de fatores:

• Requisitos específicos de segurança, confiabilidade e segurança

• Importância do ativo para a <Instituição>

• As tarefas realizadas pelo ativo

• Se o ativo é gerenciado por uma terceira parte que tem acesso ao ativo

• Se o acesso remoto ao ativo é habilitado

• O grau de confiança associado ao ativo

• Aplicar controles de cibersegurança a grupos de ativos, limitando os impactos de potenciais intrusões cibernéticas

Além disso, esses critérios devem ser claramente documentados na arquitetura de cibersegurança ou em um documento semelhante. Isso ajuda aqueles que não têm acesso ao processo original de tomada de decisão a entender por que cada critério é necessário. Por exemplo, ativos de TO que possuem características únicas (por exemplo, aqueles que dependem de softwares legados inseguros ou que possuem alta disponibilidade) podem exigir um design específico de arquitetura de cibersegurança para alcançar os objetivos operacionais da <Instituição>.

Além disso, a <Instituição> deve considerar padrões e diretrizes ao planejar a segmentação.

E12-ARQUITETURA-02-E

As proteções de rede incorporam os princípios de menor privilégio e menor funcionalidade

Detalhamento:

Segmentos de rede devem ser projetados para separar as atividades que apresentam maior risco para a <Instituição>. Por exemplo, a administração da infraestrutura de rede deve ser feita em uma rede de gerenciamento separada, restrita a contas administrativas específicas e utilizando técnicas de autenticação mais robustas, como autenticação multifator. Da mesma forma, a <Instituição> pode restringir o gerenciamento de dispositivos TO a estações de trabalho específicas na mesma rede lógica.

E12-ARQUITETURA-02-F

As proteções de rede incluem monitoramento, análise e controle do tráfego de rede para zonas de segurança selecionadas (por exemplo, firewalls, listas de permissões, sistemas de detecção e prevenção de intrusão (IDPS))

Detalhamento:

As proteções de rede incluem capacidades para monitorar, analisar e controlar o tráfego de rede. Diferentes zonas de segurança podem exigir níveis aumentados de proteção de rede com base nos requisitos de cibersegurança. Por exemplo, se a <Instituição> tiver um segmento de rede para dispositivos que se conectam via um ponto de acesso Wi-Fi convidado, o tráfego de rede pode não ser fortemente monitorado, mas haveria controle aumentado para garantir que ele não faça a transição para a rede interna. Como outro exemplo, uma rede de gerenciamento pode ser fortemente monitorada, ações realizadas na rede podem ser sujeitas a análises aumentadas, e o acesso pode ser estritamente controlado.

E12-ARQUITETURA-02-G

Tráfego web e e-mails são monitorados, analisados e controlados (por exemplo, bloqueio malicioso de links, bloqueio de downloads suspeitos, técnicas de autenticação de e-mail, bloqueio de endereços IP)

Detalhamento:

As proteções de rede devem incluir capacidades para monitorar, analisar e controlar o tráfego web e o e-mail. A web e o e-mail são vetores comuns que atacantes usam para tentar obter credenciais ou outras informações sensíveis dos usuários. Ataques de phishing e de watering hole são comumente usados para distribuir malware ou obter credenciais de usuário que são aproveitadas nos estágios iniciais da cadeia de eliminação. a <Instituição> pode considerar proteções como monitoramento de links e anexos em e-mails, quarentena de downloads suspeitos e uso de filtragem DNS para reduzir a chance de atacantes usarem esses vetores de ataque para obter uma presença na rede.

E12-ARQUITETURA-02-H

Todos os ativos são segmentados em zonas de segurança distintas de acordo com os requisitos de cibersegurança

Detalhamento:

Esta <Ação> determina que a segmentação de redes deve ser baseada em requisitos definidos de cibersegurança. Os critérios para a criação de diferentes zonas de segurança podem ser baseados em vários fatores. Estes são alguns exemplos de fatores:

• Requisitos específicos de segurança, confiabilidade e segurança

• Importância do ativo para a <Instituição>

• As tarefas realizadas pelo ativo

• Se o ativo é gerenciado por uma terceira parte

• Que tem acesso ao ativo

• Se o acesso remoto ao ativo é habilitado

• O grau de confiança associado ao ativo

• Aplicar controles de cibersegurança a grupos de ativos

• Limitando os impactos de potenciais intrusões cibernéticas

• As características da rede (por exemplo, rede sem fio de convidados)

Além disso, esses critérios devem estar claramente documentados na arquitetura de cibersegurança ou em um documento semelhante. Isso ajuda aqueles que não têm acesso ao processo original de tomada de decisão a entender por que cada critério é necessário. Por exemplo, ativos de TO que possuem características únicas (por exemplo, aqueles que dependem de softwares legados inseguros ou que possuem alta disponibilidade) podem exigir um design específico de arquitetura de cibersegurança para alcançar os objetivos operacionais da <Instituição>.

Além disso, a <Instituição> deve considerar padrões e diretrizes ao planejar a segmentação. É importante notar que existem várias formas de implementar esta <Ação>, incluindo a aplicação de um modelo zero trust.

E12-ARQUITETURA-02-I

Redes separadas são implementadas, quando necessário, que segmentam logica ou fisicamente os ativos em zonas de segurança com autenticação independente

Detalhamento:

Os requisitos de cibersegurança de certos ativos podem exigir isolamento por segmentação lógica ou física de outras redes organizacionais.

Além disso, essas redes devem incluir um esquema de autenticação independente que não seja compartilhado com outros sistemas organizacionais. uma <Instituição> pode utilizar esse tipo de segmentação para ativos críticos de TO.

E12-ARQUITETURA-02-J

Os sistemas TO são operacionalmente independentes dos sistemas de TI, permitindo que as operações TO possam ser mantidas durante uma interrupção dos sistemas de TI

Detalhamento:

Os sistemas TO devem ser arquitetados de modo que possam continuar operando quando houver uma interrupção ou interrupção nos sistemas de TI. a <Instituição> deve não apenas implementar processos manuais de backup, mas também esses processos devem ser testados para garantir que funcionem conforme esperado.

Sistemas TO referem-se a ativos que operam no segmento de rede TO. Esses ativos podem se assemelhar aos ativos tradicionais de TI, exceto que suportam operações de TO. Ao considerar esta <Ação>, esteja ciente de que sistemas de TO às vezes dependem de sistemas de TI que operam em um segmento separado da rede de TI. A intenção desta <Ação> é garantir que as atividades de entrega de

serviços ou produção suportadas pelos sistemas TO possam ser mantidas caso os sistemas de TI estejam indisponíveis por qualquer motivo.

E12-ARQUITETURA-02-K

As conexões de dispositivos à rede são controladas para garantir que apenas dispositivos autorizados possam se conectar (por exemplo, controle de acesso à rede (NAC))

Detalhamento:

As conexões de rede devem ser controladas pela <Instituição> no nível do dispositivo. Isso pode ser alcançado por meio de uma solução como o controle de acesso à rede, que não permite que dispositivos que não atendem a requisitos específicos de segurança se conectem à rede.

E12-ARQUITETURA-02-L

A arquitetura de cibersegurança permite o isolamento de ativos comprometidos

Detalhamento:

Esta <Ação> expande a implementação de táticas arquitetônicas como segmentação de rede e restrição de rede a dispositivos autorizados. A arquitetura de cibersegurança pode incluir monitoramento que permite à <Instituição> detectar se um ativo está comprometido e isolá-lo em uma rede logicamente separada. Isso poderia permitir que os respondentes realizassem análises do sistema em um ambiente seguro, sem impactar outras redes de produção.

E12-ARQUITETURA-03

Implementar a segurança de ativos de hardware de TI e TO como um elemento da arquitetura de cibersegurança

E12-ARQUITETURA-03-A

Controles lógicos e físicos de acesso são implementados para proteger ativos importantes para a entrega da <Instituição>

Detalhamento:

Os controles de cibersegurança são implementados para gerenciar os riscos associados a níveis não autorizados e/ou inadequados de acesso a TI, TO e ativos de informação, incluindo ativos físicos. Os controles lógicos podem ser administrativos (por exemplo, políticas, procedimentos), operacionais (por exemplo, manutenção do sistema, gerenciamento de capacidade) e técnicos (por exemplo, esquemas de autenticação, registro de sistemas). Os controles físicos também podem ser administrativos (por exemplo, políticas, procedimentos), operacionais (por exemplo, cercas, fechaduras, sinalização) e técnicos (por exemplo, leitores eletrônicos de crachás, detectores de movimento, registro de pontos de entrada).

E12-ARQUITETURA-03-B

Proteções de endpoints (como configuração segura, aplicações de segurança e monitoramento de host) são implementadas para proteger ativos importantes para a entrega da <Instituição>, quando possível

Detalhamento:

Proteções de endpoints referem-se a controles de cibersegurança aplicados diretamente a ativos de TI. Esses controles devem ser focados na prevenção de riscos de segurança nos endpoints, como exploits,

ataques e vazamento inadvertido de dados causado por erro humano. As proteções de endpoints podem incluir reforço de configuração, políticas e regras de configuração, software de detecção e resposta de endpoints, software anti-malware, agentes de software de monitoramento, ferramentas de prevenção de perda de dados, detecção de intrusões e firewalls baseados em host, entre outras proteções.

E12-ARQUITETURA-03-C

O princípio do privilégio mínimo (por exemplo, limitar o acesso administrativo para usuários e contas de serviço) é aplicado

Detalhamento:

As contas devem ser criadas e configuradas de acordo com o princípio do menor privilégio. O princípio do privilégio mínimo é um requisito de segurança que estabelece limitações para usuários autorizados apenas aos privilégios que eles precisam para executar tarefas atribuídas de acordo com suas responsabilidades e funções e nada mais. O princípio do menor privilégio também se aplica aos processos do sistema de informação, garantindo que os processos operem em níveis de privilégio não superiores ao necessário para cumprir as missões e/ou funções organizacionais exigidas.

No contexto desta <Ação>, é imperativo que A <Instituição> também apliquem o princípio do privilégio mínimo ao projetar, desenvolver e implementar sistemas de TI e Ordem de Gestão, garantindo que os mecanismos e controles usados para implementar o princípio do privilégio mínimo sejam viáveis e funcionem conforme projetado. O design e a construção das arquiteturas Zero Trust, por exemplo, devem estabelecer o princípio do privilégio mínimo como requisito fundamental para atingir os objetivos-chave dessa abordagem de autenticação.

E12-ARQUITETURA-03-D

O princípio da menor funcionalidade (por exemplo, limitar serviços, limitar aplicações, limitar portas, limitar dispositivos conectados) é aplicado

Detalhamento:

Os ativos devem ser configurados para fornecer apenas capacidades essenciais e restringir funcionalidades desnecessárias. Por exemplo, se um sistema estiver configurado para operar como um servidor de e-mail, portas não associadas a esse serviço devem ser fechadas e aplicações/serviços devem ser desativados caso não suportem o envio e o recebimento de e-mails.

E12-ARQUITETURA-03-E

Configurações seguras são estabelecidas e mantidas como parte do processo de implantação de ativos, sempre que possível

Detalhamento:

A configuração segura dos ativos deve ser considerada antes da implantação em um ambiente de produção, quando possível. a <Instituição> deve considerar medidas como aplicar patches, habilitar proteções baseadas em hosts, configurar o registro para suportar análises de nível mais alto e desativar contas padrão desnecessárias antes de implantar um ativo.

E12-ARQUITETURA-03-F

Aplicações de segurança são necessárias como elemento da configuração do dispositivo quando viável (por exemplo, detecção e resposta de endpoints, firewalls baseados em host)

Detalhamento:

Aplicações de segurança devem ser um elemento da configuração do dispositivo sempre que possível. a <Instituição> deve considerar proteções como soluções de detecção e resposta de endpoints que monitorem e respondam a atividades maliciosas e forneçam logs para uma plataforma de análise de nível superior. Firewalls baseados em host são outra consideração para a configuração de dispositivos, pois podem ser configurados para permitir apenas comunicação essencial.

E12-ARQUITETURA-03-G

O uso de mídias removíveis é controlado (por exemplo, limitando o uso de dispositivos USB, gerenciando discos rígidos externos)

Detalhamento:

Mídias removíveis devem ser controladas e restringidas conforme necessário para reduzir riscos. a <Instituição> pode considerar controles técnicos para restringir o uso de dispositivos removíveis em sistemas onde não há um propósito comercial, controles operacionais que restrinjam o uso de mídias removíveis por política, ou uma combinação de ambos.

E12-ARQUITETURA-03-H

Controles de cibersegurança são implementados para todos os ativos dentro da <Instituição>, seja no nível dos ativos ou como controles compensatórios quando os controles em nível de ativos não são viáveis

Detalhamento:

Esta <Ação> estende as táticas arquitetônicas para controles de cibersegurança além dos ativos importantes para a execução da <Instituição>, incluindo todos os ativos usados para a execução da <Instituição>. A <Ação> também exige que controles de cibersegurança sejam implementados no nível dos ativos, sempre que possível. Controles compensatórios devem ser implementados em situações em que um ativo não suporta controles de cibersegurança no nível do ativo para reduzir suficientemente o risco. Por exemplo, se um ativo não suportar comunicações criptografadas, nenhuma conexão direta deve ser permitida com o dispositivo e todas as comunicações devem ser roteadas por um dispositivo intermediário.

E12-ARQUITETURA-03-I

Atividades de manutenção e gestão de capacidade são realizadas para todos os ativos dentro da <Instituição>

Detalhamento:

A manutenção e a gestão de capacidade apoiam os objetivos operacionais ajudando a garantir a disponibilidade de ativos importantes para a execução da <Instituição>. a <Instituição> deve planejar a realização de manutenção adequada com o menor impacto possível nas operações. Isso pode incluir a realização de manutenção preventiva para evitar falhas inesperadas de equipamentos, bem como o agendamento da manutenção para janelas de parada planejadas ou outros horários operacionais fora do pico. O planejamento de gestão de capacidade exige compreensão das necessidades operacionais futuras da <Instituição> e orçamento, equipamentos e ferramentas adequados para atender a essas

necessidades. Isso pode exigir planejamento prévio e engajamento com processos orçamentários e liderança organizacional para desenvolver e comunicar justificativas adequadas para os recursos necessários.

E12-ARQUITETURA-03-J

O ambiente operacional físico é controlado para proteger a operação dos ativos dentro da <Instituição>

Detalhamento:

A proteção do ambiente operacional é importante para a operação contínua dos ativos usados para a execução da <Instituição>. Proteções físicas e ambientais devem ser implementadas para apoiar a sustentabilidade do ambiente operacional. A consideração desses requisitos ajudará a prevenir instabilidade da <Instituição> ou outros impactos em cascata.

E12-ARQUITETURA-03-K

Controles de cibersegurança mais rigorosos são implementados para ativos de prioridade mais alta

Detalhamento:

Ativos designados como prioridade mais alta pelo processo de priorização provavelmente apresentam um risco maior para a <Instituição> ou para o processamento de dados sensíveis e devem estar sujeitos a controles de cibersegurança mais rigorosos. A arquitetura de cibersegurança se alinhada com objetivos adicionais de segurança para ativos de maior prioridade. Exemplos de controles de cibersegurança mais rigorosos incluem monitoramento aprimorado do acesso, fatores adicionais de autenticação ou um processo de gerenciamento de mudanças com testes e aprovações adicionais.

E12-ARQUITETURA-03-L

A configuração e as mudanças no firmware são controladas ao longo do ciclo de vida do ativo

Detalhamento:

Ao longo do ciclo de vida de um ativo, pode ser necessário alterar ou atualizar o firmware por motivos como habilitar funcionalidades específicas ou melhorar o desempenho. Sempre que possível, a <Instituição> deve testar cuidadosamente as mudanças no firmware antes da implantação, pois essas mudanças também podem causar comportamentos inesperados do ativo ou de outros ativos conectados.

E12-ARQUITETURA-03-M

Controles (como listas de permissões, listas de bloqueio e configurações de configuração) são implementados para evitar a execução de código não autorizado

Detalhamento:

Além das medidas de configuração segura, a <Instituição> deve implementar controles para evitar a execução de softwares e códigos não autorizados. a <Instituição> pode usar uma política de lista de bloqueio para definir explicitamente aplicações que não são permitidas ou usar uma política de lista de permissões que especifica um conjunto limitado de aplicações permitidas.

Além disso, a <Instituição> pode optar por bloquear a execução de código como JavaScript ou macro em ativos.

E12-ARQUITETURA-04

Implementar a segurança de software como um elemento da arquitetura de cibersegurança

E12-ARQUITETURA-04-A

O software desenvolvido internamente para implantação em ativos de prioridade mais alta é desenvolvido utilizando <Ações> seguras de desenvolvimento de software

Detalhamento:

<Ações> seguras de desenvolvimento de software são codificadas em vários frameworks, como o NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM) ou o Open Web Application Security Project (OWASP). A seleção de <Ações> de desenvolvimento seguras a partir de estruturas estabelecidas deve incluir a consideração das necessidades operacionais da <Instituição>, do apetite pelo risco e do ambiente de ameaça. A segurança deve ser considerada em cada fase do ciclo de vida do desenvolvimento de software, incluindo definição de requisitos, design, desenvolvimento, testes e manutenção.

A <Instituição> também devem considerar os riscos inerentes ao uso de processos de desenvolvimento de software menos formais, como plataformas de desenvolvimento sem código. Por exemplo, sistemas de gerenciamento de conteúdo de código aberto normalmente possuem templates e outros plugins criados por terceiros que podem apresentar riscos para a <Instituição>.

E12-ARQUITETURA-04-B

A seleção do software adquirido para implantação em ativos de prioridade mais alta inclui a consideração das <Ações> seguras de desenvolvimento de software do fornecedor

Detalhamento:

A <Instituição> pode impor <Ações> seguras de desenvolvimento de software com fornecedores por diversos meios, como requisitos contratuais e testes técnicos do código do fornecedor. a <Instituição> pode especificar <Ações> seguras de design e codificação de fornecedores, como aqueles identificados em padrões estabelecidos, incluindo o NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM) e Open Web Application Security Project (OWASP). Isso pode ser feito observando o comportamento da aplicação e inferindo as <Ações> de codificação do fornecedor, ou executando alguns testes para descobrir <Ações> inseguras, como overflow de buffer, injeção SQL e autenticação ruim.

Além disso, a arquitetura de cibersegurança pode facilitar a integração e interoperabilidade dos componentes do sistema adquiridos (por exemplo, fornecendo interfaces seguras para softwares de terceiros).

Consideração adicional deve ser dada aos fornecedores de alta prioridade porque eles fornecem, mantêm ou operam componentes críticos de software essenciais para a operação da <Instituição>. A definição de um componente crítico de software pode variar amplamente dependendo da indústria ou do setor de infraestrutura crítica, e pode ser informada por frameworks ou conjuntos de controle comumente utilizados. Esta <Ação> está relacionada às atividades de arquitetura de cibersegurança associadas à seleção de fornecedores com base em suas <Ações> seguras de desenvolvimento de software.

E12-ARQUITETURA-04-C

Configurações seguras de software são necessárias como parte do processo de implantação de software tanto para softwares adquiridos quanto para softwares desenvolvidos internamente

Detalhamento:

Antes da implantação de software em um ativo, as configurações de configuração devem ser revisadas para garantir que estejam alinhadas com os requisitos de cibersegurança do ativo. A má configuração do software pode introduzir vulnerabilidades que podem ser aproveitadas por um atacante.

E12-ARQUITETURA-04-D

Todo software desenvolvido internamente é desenvolvido usando <Ações> seguras de desenvolvimento de software

Detalhamento:

Esta <Ação> exige que <Ações> seguras de desenvolvimento de software sejam utilizadas para todo software desenvolvido internamente.

E12-ARQUITETURA-04-E

A seleção de todo o software adquirido inclui a consideração das <Ações> seguras de desenvolvimento de software do fornecedor

Detalhamento:

Esta <Ação> exige que a <Instituição> considere as <Ações> de desenvolvimento de software dos fornecedores para todo o software adquirido. a <Instituição> pode especificar <Ações> seguras de design e codificação de fornecedores, como aqueles identificados em padrões estabelecidos, incluindo o NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM) e Open Web Application Security Project (OWASP).

Consideração adicional deve ser dada aos fornecedores de alta prioridade porque eles fornecem, mantêm ou operam componentes críticos de software essenciais para a operação da <Instituição>. A definição de um componente crítico de software pode variar amplamente dependendo da indústria ou do setor de infraestrutura crítica e pode ser informada por frameworks ou conjuntos de controle comumente utilizados. Esta <Ação> está relacionada às atividades de arquitetura de cibersegurança associadas à seleção de fornecedores com base em suas <Ações> seguras de desenvolvimento de software.

E12-ARQUITETURA-04-F

O processo de revisão de arquitetura avalia a segurança de aplicações novas e revisadas antes da implantação

Detalhamento:

Aplicações novas e revisadas podem introduzir mudanças nas interfaces, comportamentos e interações dos elementos arquitetônicos de cibersegurança. Tais mudanças estão sujeitas à revisão e aprovação por um conselho de revisão de arquitetura ou entidade organizacional autoritativa similar.

E12-ARQUITETURA-04-G

A autenticidade de todo o software e firmware é validada antes da implantação

Detalhamento:

A autenticidade do software, especialmente do software baixado da internet, deve ser verificada antes da execução nos sistemas organizacionais. A autenticidade do software pode ser verificada garantindo que ele seja assinado digitalmente ou comparando um hash do software com um publicado pelo fornecedor. O firmware deve ser verificado quanto à autenticidade por meio de etapas semelhantes, como comparar um hash do binário com um fornecido pelo fornecedor.

E12-ARQUITETURA-04-H

Testes de segurança (por exemplo, testes estáticos, testes dinâmicos, testes de fuzz, testes de penetração) são realizados periodicamente e de acordo com gatilhos definidos para aplicações desenvolvidas internamente e personalizadas, como mudanças no sistema e eventos externos

Detalhamento:

Os testes de segurança de software fornecem validação e verificação de que o software funciona conforme esperado em condições normais de operação e não contém fraquezas de controle ou vulnerabilidades que possam representar riscos adicionais para a <Instituição>.

Testes de segurança devem ser considerados em cada fase do ciclo de vida do desenvolvimento de software, incluindo definição de requisitos, design, desenvolvimento, testes e manutenção.

E12-ARQUITETURA-05

Implementar a segurança de dados como um elemento da arquitetura de cibersegurança

E12-ARQUITETURA-05-A

A infraestrutura de gerenciamento de chaves (ou seja, geração de chaves, armazenamento de chaves, destruição de chaves, atualização e revogação de chaves) é implementada para suportar controles criptográficos

Detalhamento:

Exemplos de táticas arquitetônicas para gerenciamento de pares e certificados de chaves público/privadas incluem armazenamentos de chaves suportados por sistemas operacionais e navegadores, servidores de chaves remotos, além de tokens criptográficos e cartões inteligentes. A manutenção da infraestrutura de gerenciamento de chaves inclui a consideração de mudanças tecnológicas que podem impactar a segurança (como computação quântica).

E12-ARQUITETURA-05-B

A arquitetura de cibersegurança inclui proteções contra alterações não autorizadas em software e firmware

Detalhamento:

Por exemplo, a arquitetura de cibersegurança impõe o uso de controles criptográficos, como certificados digitais, e rejeita atualizações de software ou firmware que não tenham sido assinadas criptograficamente.

E13-PROGRAMA

Gerenciamento do Programa de Cibersegurança

Resumo:

Um programa de cibersegurança é um grupo integrado de <Ações> projetadas e gerenciadas para atender aos objetivos de cibersegurança da <Instituição> ou da função. Um programa de cibersegurança pode ser implementado no nível da <Instituição> ou da função, mas uma implementação de nível superior e um ponto de vista corporativo podem beneficiar a <Instituição>, integrando <Ações> e alavancando investimentos em recursos em toda a <Instituição>.

Detalhamento:

O <Eixo> PROGRAMA é um <Eixo> focado na <Instituição>. As <Ações> descritas em <Eixos> focados na <Instituição> são frequentemente executadas como parte de um programa de toda a <Instituição> e podem ser estabelecidas e operar independentemente da função no escopo. Para explicar isso, o objetivo inicial em cada <Eixo> focado na <Instituição> está focado no estabelecimento e manutenção do programa relacionado.

A estratégia do programa de cibersegurança é estabelecida como a base do programa. Em sua forma mais simples, a estratégia do programa deve incluir uma lista de objetivos de cibersegurança e um plano para alcançá-los. Em níveis mais altos de maturidade, a estratégia do programa será mais completa e incluirá prioridades, uma abordagem de governança, estrutura e <Instituição> do programa e mais envolvimento da alta administração no desenho do programa. O patrocínio é importante para implementar o programa de acordo com a estratégia. A forma fundamental de patrocínio é fornecer recursos (pessoas, ferramentas e financiamento). Formas mais avançadas de patrocínio incluem o envolvimento visível de líderes seniores e a designação de responsabilidade e autoridade para o programa. Além disso, o patrocínio inclui apoio institucional para estabelecer e implementar políticas ou outras diretrizes institucionais para orientar o programa.

E13-PROGRAMA-01

Estabelecer uma estratégia de programa de cibersegurança

E13-PROGRAMA-01-A

A <Instituição> possui uma estratégia de programa de cibersegurança

Detalhamento:

A <Instituição> desenvolve, implementa e mantém uma estratégia de programa de cibersegurança que, em sua forma mais simples, inclui uma lista de objetivos de cibersegurança e ações, atividades e tarefas relacionadas, além de um plano para implementá-las. Para um programa baseado nesta metodologia, as áreas de atuação da estratégia podem se alinhar com <Eixos> e objetivos dela. Por exemplo, uma área de atividade seria identificar e responder a riscos cibernéticos que afetam os ativos e serviços da <Instituição>. Mais detalhes descreveriam como esta <Ação> deve ser realizada (novamente, alinhando-se com as <Ações> da metodologia, mas fornecendo mais detalhes sobre como as <Ações> devem ser implementadas na função, como o uso de um determinado quadro de gestão de risco).

E13-PROGRAMA-01-B

A estratégia do programa de cibersegurança define metas e objetivos para as atividades de cibersegurança da <Instituição>

Detalhamento:

Em sua forma mais simples, a estratégia do programa de cibersegurança deve incluir uma lista de metas e objetivos e, pelo menos, um plano de alto nível para as ações, atividades e tarefas que devem ser realizadas para alcançá-las. Esses objetivos devem apoiar a conquista e a melhoria contínua de uma postura adequada de cibersegurança e apoiar o cumprimento dos objetivos estratégicos organizacionais gerais.

Estes são exemplos de uma meta de cibersegurança e objetivos relacionados:

Meta: Minimizar o impacto dos incidentes de cibersegurança nos clientes.

Objetivos:

• Manter o compromisso com os clientes protegendo suas informações sensíveis contra riscos cibernéticos e respondendo de forma competente e adequada para minimizar o impacto quando ocorrerem incidentes.

• Apoiar a disponibilidade de serviços por meio da rápida detecção de incidentes de cibersegurança que possam levar a interrupções de serviço e respondendo rapidamente a esses eventos.

E13-PROGRAMA-01-C

A estratégia e prioridades do programa de cibersegurança estão documentadas e alinhadas com a missão da <Instituição>, seus objetivos estratégicos e o risco para infraestrutura crítica

Detalhamento:

A estratégia do programa de cibersegurança é desenvolvida como parte do planejamento estratégico de negócios da <Instituição> e aborda especificamente as ações, atividades e tarefas que devem ser realizadas para apoiar o alcance dos objetivos estratégicos da <Instituição> e para gerenciar riscos à infraestrutura crítica dentro da tolerância e apetite ao risco da <Instituição>.

E13-PROGRAMA-01-D

A estratégia do programa de cibersegurança define a abordagem da <Instituição> para fornecer supervisão e governança do programa para as atividades de cibersegurança

Detalhamento:

Governança é um processo de fornecer direção estratégica para a <Instituição>, garantindo que ela cumpra suas obrigações, gerencie adequadamente riscos e utilize de forma eficiente as finanças e os recursos humanos para garantir que o programa de cibersegurança apoie e sustente os objetivos estratégicos. A governança é focada em supervisionar o programa de cibersegurança, não em executar ou gerenciar tarefas de processo até a conclusão. Por exemplo, o processo de supervisionar a identificação, definição e inventário de ativos de alto valor é uma tarefa de governança, enquanto a execução dessas tarefas faz parte da gestão de ativos.

Supervisão e governança do programa podem ser alcançadas por meio de

• Um comitê formal de supervisão de cibersegurança

• Estabelecimento da metodologia como padrão para avaliação de programas de cibersegurança

• Identificação e documentação das áreas da <Instituição> e dos ativos que estão sob a alçada do programa de cibersegurança e daqueles que não estão

• Identificação de se a governança e a proteção de dados devem ser gerenciadas como parte do programa de cibersegurança ou separadamente

E13-PROGRAMA-01-E

A estratégia do programa de cibersegurança define a estrutura e <Instituição> do programa de cibersegurança

Detalhamento:

A estratégia do programa deve conter um organograma ou algum outro documento descritivo que inclua a estrutura do programa de cibersegurança, os papéis no programa e as atividades-chave associadas a esses papéis. Por exemplo, uma tabela pode ser usada para descrever departamentos (como o Centro de Operações de Segurança), subfunções dentro dos departamentos (como gerenciamento de vulnerabilidades), atividades da subfunção (como escanear, analisar e tratar vulnerabilidades) e, se aplicável, qualquer <Instituição> para a qual a subfunção seja terceirizada (como TI Corporativo).

E13-PROGRAMA-01-F

A estratégia do programa de cibersegurança identifica padrões e diretrizes que devem ser seguidos pelo programa

Detalhamento:

Normas ou diretrizes são identificadas para informar a implementação de <Ações> no programa de cibersegurança que terão implicações para atividades em todos os <Eixos> da metodologia. Essas podem ser simplesmente as fontes de referência consultadas pela <Instituição> ao desenvolver o plano para a execução das <Ações>. Eles devem incluir quaisquer padrões ou diretrizes exigidos pela política. Se a <Instituição> estiver usando a metodologia para orientar suas atividades do programa de cibersegurança, a metodologia pode ser uma das diretrizes identificadas na estratégia do programa.

Outros exemplos de normas e diretrizes são

• Diretrizes do National Institute of Standards and Technology (NIST) SP 800, como 800-53, 800-124, 800-61, 800-82, 800-30

• Estrutura do NIST para Melhorar a Cibersegurança em Infraestrutura Crítica (CSF)

• Modelos de segurança zero trust (por exemplo, NIST SP 800-207)

• Controle Crítico de Segurança do Centro de Segurança na Internet (CIS)

• Objetivos de Controle para Informação e Tecnologias Relacionadas (COBIT)

• <Instituição> Internacional de Padronização (ISO)

• Linguagem de Compras de Cibersegurança do DOE para Sistemas de Entrega de Energia

E13-PROGRAMA-01-G

A estratégia do programa de cibersegurança identifica quaisquer requisitos de conformidade aplicáveis que o programa deve ser atendido (por exemplo, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)

Detalhamento:

Os requisitos de conformidade são tipicamente impostos à <Instituição> por governos locais, estaduais ou federais. Requisitos de conformidade diferentes podem se aplicar a alguns, mas não a todos os ativos no escopo do programa de cibersegurança. O programa de cibersegurança deve estar ciente dos

requisitos de conformidade que o programa deve cumprir e do escopo de cada requisito. Listar os requisitos de conformidade na estratégia do programa de cibersegurança ajuda a garantir que os interessados do programa de cibersegurança saibam pelo que são responsabilizados. Por exemplo, uma estratégia pode incluir uma declaração de que a conformidade com o PCI DSS é exigida pelo programa de cibersegurança. a <Instituição> deve considerar as diferenças nos requisitos legais e regulatórios dentro das áreas em que atuam e como elas podem entrar em conflito com controles globais de TI, TI corporativa ou cibersegurança.

Alguns exemplos de requisitos de conformidade que a <Instituição> pode precisar cumprir incluem:

• Normas de Proteção de Infraestrutura Crítica (CIP) da North American Electric Reliability Corporation (NERC)

• Diretrizes de Segurança de Dutos da Administração de Segurança do Transporte (TSA)

• Normas de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS)

• <Instituição> Internacional de Padronização (ISO)

• Certificação do Modelo de Maturidade em Cibersegurança do Departamento de Defesa (DoD CMMC)

• Lei de Privacidade do Consumidor da Califórnia (CCPA)

• Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (HIPAA)

• Leis estaduais e locais de cibersegurança e privacidade

E13-PROGRAMA-01-H

A estratégia do programa de cibersegurança é atualizada periodicamente e de acordo com gatilhos definidos, como mudanças no negócio, mudanças no ambiente operacional e alterações no perfil de ameaça (AMEAÇA-2e)

Detalhamento:

A <Instituição> deve ter um processo documentado para garantir que certos tipos de mudanças desencadeiam uma atualização da estratégia do programa de cibersegurança. Um exemplo de mudança no negócio que exigiria uma atualização seria uma mudança no negócio que aumente sua exposição a eventos cibernéticos, como a entrada em uma nova linha de negócios. Um exemplo de mudança no ambiente operacional que pode exigir uma atualização seria a aquisição de um novo sistema de gestão de clientes que utilize informações sensíveis. Um exemplo de mudança no perfil de ameaça de uma empresa de serviços públicos que pode exigir uma atualização seria o relatório de ameaças, que indica aumento da atividade de ciberataques direcionados a utilitários.

E13-PROGRAMA-02

Estabelecer e manter o programa de cibersegurança

E13-PROGRAMA-02-A

A alta gerência com autoridade adequada oferece suporte ao programa de cibersegurança, pelo menos de forma pontual

Detalhamento:

Contar com apoio material da alta administração é necessário para implementar um programa de cibersegurança. As formas fundamentais de apoio são fornecer recursos (pessoas, ferramentas e

financiamento) e autoridade para realizar atividades de cibersegurança. Para fornecer esse apoio, os próprios gerentes seniores devem ter autoridade suficiente e relevante.

E13-PROGRAMA-02-B

O programa de cibersegurança é estabelecido de acordo com a estratégia do programa de cibersegurança

Detalhamento:

O programa de cibersegurança é normalmente responsável por garantir que os objetivos de cibersegurança, conforme documentados na estratégia do programa, sejam alcançados. Por exemplo, o programa de cibersegurança inclui atividades para garantir que equipe adequada esteja disponível para cumprir os requisitos da estratégia do programa.

E13-PROGRAMA-02-C

O patrocínio da alta administração para o programa de cibersegurança é visível e ativo

Detalhamento:

O patrocínio visível e ativo da alta administração pode incluir comunicações regulares da alta administração sobre a importância e o valor das atividades de cibersegurança, apoio organizacional para estabelecer e implementar políticas ou outras diretrizes organizacionais para orientar o programa, financiamento de prêmios e programas de reconhecimento para funcionários que contribuem significativamente para alcançar os objetivos de cibersegurança, e a garantia de que conceitos de cibersegurança sejam incluídos em contratos com Fornecedores e parceiros de negócios.

E13-PROGRAMA-02-D

O patrocínio da alta gestão é fornecido para o desenvolvimento, manutenção e aplicação de políticas de cibersegurança

Detalhamento:

As políticas são uma expressão do nível de compromisso dos altos gestores com o programa de cibersegurança. A falta de endosso visível das políticas de cibersegurança por parte dos altos gerentes normalmente torna as políticas menos eficazes, pois as partes interessadas podem assumir que as políticas não estão sendo aplicadas ou que são apenas usadas como diretrizes e não como exigência. Os gerentes seniores devem comunicar a importância das políticas de cibersegurança para a missão e o bem-estar da <Instituição> e expressar sua intenção de responsabilizar as partes interessadas pela conformidade.

E13-PROGRAMA-02-E

A responsabilidade pelo programa de cibersegurança é atribuída a um cargo com autoridade suficiente

Detalhamento:

É importante que o papel responsável pela execução do programa de cibersegurança (como um diretor de segurança da informação) tenha a autoridade necessária e suficiente dentro da <Instituição> para realizar as atividades do programa e obter os recursos necessários para apoiá-lo.

E13-PROGRAMA-02-F

Os interessados nas atividades de gestão de programas de cibersegurança são identificados e envolvidos

Detalhamento:

Os stakeholders do programa de cibersegurança são identificados e envolvidos na execução das <Ações>. Isso pode incluir partes interessadas de dentro da <Instituição>, de toda a <Instituição> ou de fora dela, dependendo de como a <Instituição> implementou as <Ações>. Os stakeholders podem incluir gerentes de projeto, proprietários de processos de negócios e proprietários de ativos e serviços afetados, bem como funcionários envolvidos em atividades de cibersegurança. A identificação das partes interessadas e seu envolvimento adequado deve ser documentada de alguma forma, como em descrições de cargos ou estatutos de equipe.

E13-PROGRAMA-02-G

As atividades do programa de cibersegurança são periodicamente revisadas para garantir que estejam alinhadas com a estratégia do programa de cibersegurança

Detalhamento:

Deveria haver um processo para avaliar periodicamente as atividades do programa de cibersegurança, garantindo que continuem apoiando os objetivos e metas da estratégia do programa de cibersegurança. Atividades que não contribuem para o cumprimento desses objetivos devem ser avaliadas para determinar se devem continuar. Quaisquer lacunas no cumprimento dos objetivos também devem ser abordadas.

E13-PROGRAMA-02-H

As atividades de cibersegurança são revisadas de forma independente para garantir conformidade com políticas e procedimentos de cibersegurança, periodicamente e de acordo com gatilhos definidos, como mudanças de processos

Detalhamento:

O objetivo desta <Ação> é fornecer garantia adicional de que as atividades de cibersegurança estão sendo realizadas conforme especificado pelas políticas e procedimentos de cibersegurança da <Instituição>. A avaliação deve ser independente; ou seja, conduzidos por revisores externos ao programa de cibersegurança sob a direção do órgão governante da <Instituição>). Aqueles diretamente envolvidos nas atividades do programa não podem realizar a avaliação nem emitir uma opinião sobre a eficácia do programa. Tais avaliações podem ser realizadas por meio de auditorias internas e externas, revisões pós-evento e avaliações de capacidade, e devem ser iniciadas e responsáveis perante o conselho diretor ou um grupo similar. Técnicas avançadas de cibersegurança, como caça a ameaças e defesa ativa, podem ser usadas para fornecer insights sobre o desempenho do programa geral de cibersegurança.

E13-PROGRAMA-02-I

O programa de cibersegurança aborda e possibilita a obtenção de conformidade legal e regulatória, conforme apropriado

Detalhamento:

A <Instituição> deve ter profissionais responsáveis por garantir que esteja ciente de todas as obrigações de conformidade regulatória às quais está sujeita por parte de governos e outras fontes. Os objetivos do programa de cibersegurança devem estar alinhados e apoiar o cumprimento de quaisquer dessas obrigações relevantes para a cibersegurança, e o programa deve desenvolver e implementar os procedimentos e atividades adequados para garantir o cumprimento de maneira rápida e precisa.

E13-PROGRAMA-02-J

A <Instituição> colabora com entidades externas para contribuir para o desenvolvimento e implementação de padrões, diretrizes, <Ações> líderes, lições aprendidas e tecnologias emergentes de cibersegurança

Detalhamento:

Além de manter a consciência de quaisquer padrões de cibersegurança do setor aos quais a <Instituição> seja obrigada a cumprir (como o padrão de Proteção de Infraestrutura Crítica da North American Energy Reliability Corporation), a <Instituição> deve atribuir responsabilidade a profissionais selecionados para contribuir com os esforços da indústria para desenvolver <Ações> ou diretrizes de cibersegurança. Por exemplo, as <Ações> da Indústria de Cartões de Pagamento foram desenvolvidas por partes interessadas do setor de cartões de crédito para implementação voluntária.

E14-SUSTENTAÇÃO

Gestão do Ciclo de Vida de Ativos

Resumo:

Estabelecer um programa de gestão do ciclo de vida de ativos, considerando as fases de planejamento da aquisição, aquisição, implantação, operação, manutenção, atualização, suporte e descarte, envolve identificar os requisitos de cibersegurança reduzindo ameaças e vulnerabilidades para os ativos da <Instituição> e projetar controles apropriados para protegê-los.

Detalhamento:

O <Eixo> SUSTENTAÇÃO tem por objetivo a gestão do ciclo de vida dos ativos, constituindo uma abordagem estratégica que supervisiona e controla os ativos de hardware e software da <Instituição>, desde o momento em que sua necessidade é identificada até a sua retirada definitiva do uso. Seu objetivo é maximizar o valor de negócio dos ativos, otimizar custos, garantir a conformidade legal, assegurar a qualidade da entrega dos serviços dependentes de tecnologia e evitar vulnerabilidades decorrentes da má gestão dos ativos.

Por praticidade, o <Eixo> SUSTENTAÇÂO foi subdividido em fases distintas do ciclo de vida dos ativos, que demandam <Processos> e <Ações> específicas.

A fase de Planejamento da Aquisição é uma etapa analítica onde se identificam as demandas do negócio e se definem os requisitos técnicos e orçamentários. O foco geralmente é a padronização de tecnologias e a verificação de estoques ou licenças existentes (reuso) para evitar compras desnecessárias e projetar o Custo Total de Propriedade (TCO) antes da aprovação do investimento.

A fase de Aquisição corresponde à execução da compra e recebimento dos ativos, que engloba a negociação com fornecedores, a gestão contratual e a entrada fiscal. É neste momento que ocorre o registro inicial no inventário (tombamento), estabelecendo formalmente o início da responsabilidade da <Instituição> sobre o bem.

A fase de Implantação corresponde ao processo técnico de preparação do ativo para uso produtivo, que inclui a configuração de imagens de sistema, instalação de aplicativos, aplicação de políticas de segurança e a entrega física ou lógica ao usuário final, garantindo que o recurso esteja pronto para operar conforme os padrões da empresa.

A fase de Operação refere-se ao cotidiano do ativo em funcionamento no ambiente corporativo. O foco desta fase é o monitoramento contínuo da disponibilidade, capacidade e utilização dos recursos, assegurando que o hardware e o software entreguem o desempenho esperado para sustentar os processos de negócio. Essa fase geralmente corresponde de 70% a 90% do ciclo de vida dos ativos.

A Manutenção, que na prática ocorre durante a fase de Operação do ativo, constitui o conjunto de intervenções técnicas (preventivas ou corretivas) destinadas a preservar a integridade do ativo. Envolve reparos físicos, substituição de peças desgastadas e correções de bugs, visando evitar paradas não planejadas e garantir que o ativo cumpra sua vida útil estimada.

A Atualização também ocorre durante a fase de Operação do ativo, e corresponde a ações proativas para modernizar o ativo e mantê-lo seguro e eficiente. Inclui a aplicação de patches de segurança, instalação de novas versões de software e upgrades de hardware (como aumento de memória), protegendo o ambiente contra vulnerabilidades e obsolescência tecnológica.

O Suporte consiste no serviço de assistência direta aos usuários para resolver incidentes e dúvidas relacionadas aos ativos. Atua como a linha de frente para restabelecer o serviço rapidamente em caso de falhas, garantindo que a produtividade do usuário não seja comprometida por questões técnicas.

A fase de Descarte é aquela final e crítica que encerra o ciclo de vida. Envolve a sanitização segura de dados (para evitar vazamento de informações), o cancelamento de contratos de licença e a destinação ambientalmente correta do lixo eletrônico (e-waste), seguida da baixa contábil e remoção do registro no sistema de inventário.

E14-SUSTENTAÇÃO-01

Atividades de planejamento da aquisição de ativos

E14-SUSTENTAÇÃO-01-A

As aquisições de ativos são planejadas

Detalhamento:

O Planejamento da Aquisição é uma etapa analítica onde se identificam as demandas do negócio e se definem os requisitos técnicos e orçamentários. O foco geralmente é a padronização de tecnologias e a verificação de estoques ou licenças existentes (reuso) para evitar compras desnecessárias e projetar o Custo Total de Propriedade (TCO) antes da aprovação do investimento.

E14-SUSTENTAÇÃO-01-B

São estabelecidos prazos máximos para decisão sobre renovação de licenciamento de software

Detalhamento:

A <Instituição> estabelece procedimentos para decidir sobre a necessidade de renovação do licenciamento de um software ou pela substituição do software em função do encerramento da validade do licenciamento.

A ausência de prazos máximos para a tomada de decisão sobre renovações resulta na expiração de licenças. Quando uma licença expira, o fornecedor interrompe o envio de patches e atualizações críticas de segurança, transformando o ativo em um software legado vulnerável a exploits de dia zero (zero-day).

Além disso, sistemas não renovados podem bloquear o acesso dos usuários repentinamente, interrompendo operações críticas, ou violar direitos de propriedade intelectual, gerando sanções jurídicas e financeiras. Estreitar essa janela temporal por meio de prazos formais garante que a governança de TI antecipe as negociações, mantendo a integridade, a conformidade legal e o suporte contínuo contra ameaças cibernéticas.

E14-SUSTENTAÇÃO-02

Atividades de aquisição de ativos

E14-SUSTENTAÇÃO-02-A

As aquisições são realizadas de forma sistematizada

Detalhamento:

A Aquisição corresponde à execução da compra e recebimento dos ativos, que engloba a negociação com fornecedores, a gestão contratual e a entrada fiscal. É neste momento que ocorre o registro inicial no inventário (tombamento), estabelecendo formalmente o início da responsabilidade da <Instituição> sobre o bem.

A aquisição sistematizada garante que nenhum software, hardware ou serviço em nuvem entre na <Instituição> sem passar por uma homologação prévia de segurança. Isso mitiga riscos de espionagem

industrial, vulnerabilidades herdadas em códigos de terceiros e a introdução de malwares na rede corporativa através de compras avulsas realizadas por setores independentes (a chamada Shadow IT).

O processo sistematizado estabelece critérios técnicos de triagem, due diligence do fornecedor e análise de conformidade legal antes do fechamento do contrato, blindando o perímetro operacional contra ameaças originadas na cadeia de suprimentos.

E14-SUSTENTAÇÃO-02-B

São estabelecidos prazos máximos para renovação de licenciamento de software

Detalhamento:

A <Instituição> estabelece os prazos máximos para renovação do licenciamento ou substituição do software em uso de tal forma que não ultrapasse a data de encerramento da validade do de seu licenciamento.

Softwares com licenciamento expirado perdem o direito a atualizações de segurança e correções de bugs (patches) fornecidas pelo fabricante. Isso transforma o ativo em um sistema legado vulnerável, tornando-o alvo fácil para explorações automatizadas, malwares e invasões.

Estabelecer prazos máximos para a tomada de decisão de renovação garante a continuidade do suporte de segurança e mitiga riscos financeiros e de conformidade legal (direitos autorais). O prazo estrito impede o "vazio de proteção" — o período crítico entre o vencimento da licença antiga e a aprovação burocrática da nova —, blindando a infraestrutura contra brechas decorrentes de negligência administrativa.

E14-SUSTENTAÇÃO-02-C

Ativos de software sem licenciamento válido são marcados como "não-autorizado"

Detalhamento:

A <Instituição> marca como não-autorizado qualquer software sem licenciamento válido, bloqueando seu uso e definindo os procedimentos de tratamento que deverão ser adotados, dentre eles: remoção do software, negação de acesso ao software ou quarentena do software.

A marcação de softwares sem licença válida como "não-autorizado" justifica-se por três fatores críticos de risco:

• Vulnerabilidade Técnica: Softwares não licenciados perdem o suporte do fabricante e deixam de receber patches de segurança, violando o controle de correção de falhas (NIST SI-2).

• Superfície de Ataque: Aplicativos piratas ou sem conformidade frequentemente servem de vetor para malwares e backdoors introduzidos por ativadores ilegais (cracks).

• Conformidade Legal: Evita sanções civis e criminais por violação de direitos autorais (ISO 27002 5.32).

Essa classificação aciona o isolamento automático do ativo por ferramentas de gerenciamento (SAM/EDR), mitigando riscos antes que comprometam a rede.

E14-SUSTENTAÇÃO-03

Atividades de implantação de ativos

E14-SUSTENTAÇÃO-03-A

A implantação de ativos segue procedimentos definidos

Detalhamento:

A Implantação corresponde ao processo técnico de preparação do ativo para uso produtivo, que inclui a configuração de imagens de sistema, instalação de aplicativos, aplicação de políticas de segurança e a entrega física ou lógica ao usuário final, garantindo que o recurso esteja pronto para operar conforme os padrões da empresa.

A justificativa para se exigir procedimentos definidos na implantação de ativos visa mitigar os riscos de vulnerabilidades decorrentes de configurações padrão vulneráveis, introdução de artefatos maliciosos e desalinhamento com a arquitetura de segurança da <Instituição>.

Sem um processo padronizado, a esteira de produção fica exposta a falhas humanas e implantações ad-hoc que comprometem a integridade do ambiente, dificultam a rastreabilidade por auditorias e geram pontos cegos no inventário de ativos. A padronização garante a aplicação consistente de hardening, testes de segurança prévios e a devida autorização formal antes da entrada em operação.

E14-SUSTENTAÇÃO-04

Atividades de operação de ativos

E14-SUSTENTAÇÃO-04-A

A operação dos ativos é sistematizada

Detalhamento:

A Operação refere-se ao cotidiano do ativo em funcionamento no ambiente corporativo. O foco desta fase é o monitoramento contínuo da disponibilidade, capacidade e utilização dos recursos, assegurando que o hardware e o software entreguem o desempenho esperado para sustentar os processos de negócio. Essa fase geralmente corresponde de 70% a 90% do ciclo de vida dos ativos.

Esta <Ação> exige a documentação formal, automação e homologação de todas as rotinas diárias, como backups, aplicação de patches e provisionamento de recursos.

A justificativa de sua existência reside na eliminação da dependência de conhecimento tácito ("cultura do herói") e na mitigação de erros humanos decorrentes de execuções ad-hoc. A sistematização garante a repetibilidade dos processos, assegura que modificações nos ativos passem por fluxos de aprovação e auditoria, e mantém o ambiente técnico em um estado conhecido e seguro. Isso reduz drasticamente incidentes causados por configurações incorretas e acelera o tempo de recuperação em caso de falhas operacionais.

E14-SUSTENTAÇÃO-05

Atividades de manutenção de ativos

E14-SUSTENTAÇÃO-05-A

A manutenção de ativos é sistematizada

Detalhamento:

A Manutenção constitui o conjunto de intervenções técnicas (preventivas ou corretivas) destinadas a preservar a integridade do ativo. Envolve reparos físicos, substituição de peças desgastadas e correções de bugs, visando evitar paradas não planejadas e garantir que o ativo cumpra sua vida útil estimada.

A sistematização da manutenção de ativos justifica-se pela necessidade de eliminar a imprevisibilidade operacional e mitigar riscos cibernéticos. Sem um processo padronizado e automatizado, a <Instituição> perde a visibilidade sobre obsolescência tecnológica, expiração de licenças e componentes não autorizados na rede.

Mapear e manter ativos de forma sistêmica garante que vulnerabilidades sejam identificadas proativamente (vinculadas ao controle de correção de falhas) e que patches de segurança sejam aplicados uniformemente. Além disso, estabelece uma linha de base (baseline) confiável para a resposta a incidentes, permitindo a rápida contenção de ameaças ao correlacionar alertas com o proprietário e a criticidade do ativo afetado, blindando a continuidade do negócio.

E14-SUSTENTAÇÃO-06

Atividades de atualização de ativos

E14-SUSTENTAÇÃO-06-A

Ativos descontinuados ou sem suporte são substituídos

Detalhamento:

A <Instituição> estabelece procedimentos para a substituição de ativos nos casos de encerramento de produção (descontinuação) e definição de data de encerramento do suporte oficial por parte do fornecedor.

Fabricantes deixam de mitigar brechas de segurança e de lançar patches de correção quando um ativo atinge o fim da vida útil (End of Life - EOL). Manter sistemas descontinuados na rede cria uma vulnerabilidade permanente, tornando-os alvos fáceis para exploração automatizada, malware e ataques cibernéticos.

A substituição obrigatória garante a conformidade com o Princípio da Atualização Contínua, preserva a integridade e a disponibilidade do ambiente tecnológico e assegura que todos os componentes da infraestrutura possuam suporte técnico ativo para responder a novas ameaças.

E14-SUSTENTAÇÃO-06-B

A atualização tecnológica dos ativos é sistematizada

Detalhamento:

Manter ativos obsoletos ou sem correções expõe a infraestrutura a vulnerabilidades conhecidas, exploradas por malwares e atacantes. A obsolescência também encerra o suporte do fabricante, interrompendo patches de segurança. Ao sistematizar o ciclo de vida e a aplicação de atualizações, a <Instituição> mitiga riscos de forma proativa, assegura a continuidade do negócio, mantém a conformidade legal e protege a integridade e confidencialidade dos dados contra ameaças cibernéticas emergentes.

E14-SUSTENTAÇÃO-07

Atividades de suporte aos usuários dos ativos

E14-SUSTENTAÇÃO-07-A

Os ativos em uso têm suporte técnico

Detalhamento:

A <Instituição> assegura que os ativos em uso dispõem de suporte técnico prestado pelo fabricante, distribuidor ou empresa especializada.

Softwares e hardwares sem suporte técnico ativo (conhecidos como End-of-Life ou Legacy) deixam de receber atualizações de segurança e correções de código (patches) por parte do fabricante. Quando novas vulnerabilidades são descobertas nesses ativos obsoletos, elas permanecem abertas indefinidamente, criando uma porta de entrada permanente para invasões, infecções por malwares e vazamento de dados.

Portanto, exigir suporte técnico ativo garante a continuidade do fornecimento de correções cibernéticas, mitigando os riscos operacionais e assegurando a conformidade legal e a integridade da infraestrutura tecnológica da <Instituição>.

E14-SUSTENTAÇÃO-07-B

Apenas ativos com suporte são classificados com "autorizado"

Detalhamento:

A <Instituição> assegura que apenas ativos com suporte sejam classificados como "autorizado" no inventário de ativos.

Ativos descontinuados pelo fabricante (End-of-Support / End-of-Life) deixam de receber atualizações de segurança e correções de falhas. Isso significa que novas vulnerabilidades descobertas nesses componentes nunca serão corrigidas, tornando-os alvos fáceis para invasões e malwares.

Classificar um ativo como "autorizado" dentro do inventário corporativo implica que a <Instituição> consegue garantir sua integridade e segurança. Se um dispositivo ou sistema não possui mais suporte técnico, o risco de segurança associado torna-se inaceitável e impossível de ser mitigado de forma nativa.

Portanto, a regra garante a conformidade operacional e impede a exposição da rede, forçando a substituição ou segregação de tecnologias obsoletas antes que se tornem vetores de ataque comprometedores.

E14-SUSTENTAÇÃO-07-C

Apenas software licenciados são classificados com "autorizado"

Detalhamento:

A <Instituição> assegura que apenas softwares com licenciamento válido são classificados como "autorizado" no inventário de ativos.

Classificar apenas softwares licenciados como "autorizados" é uma medida crítica de mitigação de riscos por três motivos fundamentais:

• Garantia de Atualizações (Segurança): Softwares não licenciados ou piratas não recebem patches oficiais do fabricante, violando o controle de correção de falhas e deixando o sistema vulnerável a exploits e malwares.

• Prevenção de Ameaças Ocultas: Instaladores sem licença válida obtidos fora dos canais oficiais frequentemente contêm cavalos de troia e spywares acoplados para burlar a validação do produto.

• Conformidade Legal e Integridade: Garante a governança de TI, evitando sanções jurídicas e financeiras por violação de direitos autorais, assegurando que apenas aplicações homologadas e com suporte técnico ativo processem os dados organizacionais.

E14-SUSTENTAÇÃO-07-D

Ativos sem suporte, mas necessários à <Instituição> são classificados como "exceção"

Detalhamento:

A <Instituição> documenta como exceção o uso de qualquer ativo sem suporte, mas que seja necessário para o cumprimento das atividades da <Instituição>, detalhando os controles de mitigação adotados, o risco residual da situação, e o responsável pela autorização de uso do ativo.

Classificar ativos sem suporte como "exceção" é um controle formal necessário porque softwares ou hardwares legados que perderam o suporte do fabricante não recebem mais atualizações e correções de vulnerabilidades. Isso cria uma brecha permanente na segurança da informação.

Ao formalizar o ativo como uma exceção no inventário de conformidade, a <Instituição> justifica sua necessidade para a continuidade do negócio e, obrigatoriamente, implementa controles compensatórios (como isolamento de rede, monitoramento estrito por SIEM ou execução em ambientes virtuais restritos). Esse processo garante a aprovação explícita e assinada da alta gestão (aceitação de risco), transferindo a responsabilidade legal e operacional e impedindo que o ativo desatualizado passe despercebido pelas auditorias de segurança.

E14-SUSTENTAÇÃO-07-E

Ativos sem suporte, não marcados como "exceção", são classificados como "não-autorizado"

Detalhamento:

A <Instituição> documenta como não-autorizado qualquer ativo sem suporte para o qual não for documentada uma exceção, bloqueando seu uso e definindo os procedimentos de tratamento que deverão ser adotados, dentre eles: descarte do ativo, negação de acesso ao ativo ou quarentena do ativo.

Ativos de software ou hardware que perderam o suporte do fabricante deixam de receber atualizações de segurança, tornando-se vetores críticos para a introdução de malwares e invasões. Ao classificá-los automaticamente como "não-autorizados", a <Instituição> força a visibilidade do risco e impede a negligência operacional.

A marcação de "exceção" é o único mecanismo legítimo de governança, exigindo uma análise de risco formal, aprovação dos proprietários dos dados e a implementação de controles compensatórios (como segregação de rede ou monitoramento estrito). Sem essa justificativa documentada, a permanência do ativo sem suporte constitui uma violação de conformidade, acionando o bloqueio automatizado ou o isolamento imediato do dispositivo para proteger o ecossistema corporativo.

E14-SUSTENTAÇÃO-08

Atividades de descarte de ativos

E14-SUSTENTAÇÃO-08-A

São estabelecidos prazos máximos para descarte de ativos com suporte encerrado

Detalhamento:

A <Instituição> estabelecer prazos máximos para descarte de ativos em função do encerramento oficial de seu suporte pelo fornecedor, caso não seja possível contratar suporte estendido do fornecedor para o ativo para além da data do fim do suporte oficial.

A regra de prazo máximo para descarte justifica-se pela mitigação de riscos cibernéticos e de conformidade. Ativos com suporte encerrado (End-of-Support - EOS) deixam de receber atualizações de segurança e correções de vulnerabilidades (patches). Manter esses itens na infraestrutura — ou mesmo armazenados de forma negligente — cria pontos cegos exploráveis por atacantes para movimentação lateral na rede.

Estabelecer um prazo limite força a <Instituição> a substituir ou descartar o dispositivo/software de forma segura, evitando a janela de exposição a ameaças de "dia zero". Além disso, o controle garante a conformidade legal e regulatória (como LGPD/GDPR), pois ativos obsoletos falham em auditorias devido à incapacidade técnica de garantir a confidencialidade e a integridade dos dados trafegados.

E14-SUSTENTAÇÃO-08-B

São estabelecidos prazos máximos para descarte de ativos descontinuados

Detalhamento:

A <Instituição> estabelece os prazos máximos para o descarte de todo ativo descontinuado pelo fornecedor de tal forma que não ultrapasse a data do encerramento oficial de seu suporte oficial.

Manter ativos descontinuados (hardwares ou softwares obsoletos) no inventário sem um prazo limite para descarte gera duas vulnerabilidades críticas: aumento da superfície de ataque e vazamento de dados. Equipamentos antigos deixam de receber atualizações de segurança, tornando-se alvos fáceis para invasores que os utilizam como porta de entrada para a rede corporativa. Além disso, o armazenamento prolongado e descontrolado de mídias antigas eleva o risco de perda ou roubo físico de informações confidenciais.

Ao estabelecer um prazo máximo de descarte, o controle garante a destruição segura dos dados, reduz custos operacionais de armazenamento e elimina pontos cegos na infraestrutura, mantendo o ambiente em conformidade legal com regulamentações de privacidade.

E14-SUSTENTAÇÃO-08-C

O descarte de ativos é sistematizado

Detalhamento:

O Descarte é a fase final e crítica que encerra o ciclo de vida. Envolve a sanitização segura de dados (para evitar vazamento de informações), o cancelamento de contratos de licença e a destinação ambientalmente correta do lixo eletrônico (e-waste), seguida da baixa contábil e remoção do registro no sistema de inventário.

Ativos descartados de forma comum ou desorganizada mantêm fragmentos de dados que podem ser recuperados por engenharia reversa ou técnicas forenses.

Equipamentos mal descartados mantêm fragmentos de dados recuperáveis. Paralelamente, o descarte de softwares e licenças sem controle sistêmico resulta em desperdício financeiro por subutilização, riscos legais por violação de propriedade intelectual e brechas de segurança, como instâncias órfãs em nuvem ou softwares descontinuados sem atualizações (end-of-life).

A sistematização garante um processo auditável que executa a destruição física ou sanitização lógica do hardware, além da revogação formal de acessos, desinstalação de sistemas e devolução de licenças

ao inventário (de-provisioning). Isso protege segredos comerciais e assegura a conformidade regulatória (como a LGPD) em todo o ciclo de vida dos ativos.

A sistematização garante um processo auditável que aplica métodos formais de desmagnetização, destruição física ou sanitização lógica completa (criptografia e purging), permitindo a emissão de certificados oficiais de destruição. Esse rigor mitiga riscos legais, financeiros e de reputação, impedindo que segredos comerciais, credenciais ou dados de clientes caiam nas mãos de terceiros após o fim do ciclo de vida do ativo.