Cibersegurança

Topical Requirement

Requisito Temático

Guia do Usuário

The Institute of
Internal Auditors

Conteúdo

Visão Geral dos Requisitos Temáticos

Os Requisitos Temáticos são um componente essencial do Framework Internacional de Práticas Profissionais (International Professional Practices Framework®), juntamente com as Normas Globais de Auditoria Interna (Global Internal Audit Standards™) e as Orientações Globais. The Institute of Internal Auditors exige que os Requisitos Temáticos sejam usados em conjunto com as Normas Globais de Auditoria Interna, que fornecem a base fidedigna para as práticas exigidas. Referências às Normas aparecem ao longo deste guia como fonte de informações mais detalhadas.

Os Requisitos Temáticos formalizam como os auditores internos abordam as áreas de risco predominantes para promover a qualidade e a consistência dentro da profissão. Os Requisitos Temáticos estabelecem uma linha de base e fornecem critérios relevantes para a realização de serviços de auditoria relacionados ao assunto de um Requisito Temático (Norma 13.4 - Critérios de Avaliação). A conformidade com os Requisitos Temáticos é obrigatória para serviços de avaliação e recomendadas para análise durante serviços de consultoria. Os Requisitos Temáticos não têm a intenção de abranger todos os aspectos potenciais que deveriam ser considerados na execução de trabalhos de avaliação; ao contrário, têm a intenção de fornecer um conjunto mínimo de requisitos para permitir uma avaliação consistente e confiável do tema.

Os Requisitos Temáticos estão claramente vinculados ao Modelo das Três Linhas do The IIA e às Normas Globais de Auditoria Interna. Os processos de governança, gerenciamento de riscos e controle são os principais componentes dos Requisitos Temáticos, alinhados à Norma 9.1 – Entendendo os processos de governança, gerenciamento de riscos e controle. Em referência ao Modelo das Três Linhas, a governança está ligada ao conselho/órgão de governança, o gerenciamento de riscos está ligado à segunda linha e os controles ou processos de controle estão ligados à primeira linha. Embora a gestão esteja representada tanto na primeira quanto na segunda linha, a função de auditoria interna está representada na terceira linha, como prestadora independente e objetiva de avaliação, reportando ao conselho/órgão de governança (Princípio 8: Supervisionado pelo Conselho).

Aplicabilidade, Risco e Julgamento Profissional

Os Requisitos Temáticos devem ser seguidos quando as funções de auditoria interna realizam trabalhos de avaliação sobre assuntos para os quais existe um Requisito Temático, ou quando aspectos do Requisito Temático são identificados em outros trabalhos de avaliação.

Conforme descrito nas Normas, avaliar os riscos é uma parte importante do planejamento do chefe executivo de auditoria. A determinação dos trabalhos de avaliação a serem

incluídos no plano de auditoria interna requer a avaliação das estratégias, objetivos e riscos da organização pelo menos anualmente (Norma 9.4 - Plano de Auditoria Interna). Ao planejar trabalhos de avaliação individuais, os auditores internos devem avaliar os riscos relevantes para o trabalho (Norma 13.2 - Avaliação de Risco do Trabalho).

Quando o assunto de um Requisito Temático for identificado durante o processo de planejamento de auditoria interna baseado em riscos e for incluído no plano de auditoria, os requisitos descritos no Requisito Temático devem ser usados para avaliar o tema nos trabalhos aplicáveis. Além disso, quando os auditores internos realizam um trabalho (incluído ou não no plano) e surgem elementos de um Requisito Temático, sua aplicabilidade como parte do trabalho deve ser avaliada. Por fim, se for solicitado um trabalho que não estava originalmente no plano e incluir o tema, a aplicabilidade do Requisito Temático deve ser avaliada.

O julgamento profissional desempenha um papel fundamental na aplicação do Requisito Temático. As avaliações de riscos orientam as decisões dos chefes executivos de auditoria sobre quais trabalhos incluir no plano de auditoria interna (Norma 9.4 - Plano de Auditoria Interna). Além disso, os auditores internos usam o julgamento profissional para determinar quais aspectos serão cobertos em cada trabalho (Normas 13.3 - Objetivos e Escopo do Trabalho, 13.4 - Critérios de Avaliação e 13.6 - Programa de Trabalho). O Anexo A "Exemplos de Aplicação Prática" descreve como os auditores internos determinam se o Requisito Temático se aplica.

As evidências de que a aplicabilidade de cada requisito do Requisito Temático foi avaliada devem ser guardadas, incluindo uma justificativa que explique a exclusão de quaisquer requisitos. A conformidade com o Requisito Temático deve ser documentada usando o julgamento profissional do auditor, conforme descrito na Norma 14.6 - Documentação do Trabalho.

Embora o Requisito Temático de Cibersegurança forneça uma linha de base de processos de controle a serem considerados, organizações que avaliam o risco cibernético como muito alto podem precisar avaliar aspectos adicionais.

Se um chefe executivo de auditoria determinar que a função de auditoria interna não tem o conhecimento necessário para realizar trabalhos de auditoria sobre um assunto de Requisito Temático, o trabalho de auditoria pode ser terceirizado (Normas 3.1 - Competência, 7.2 - Qualificações do Chefe Executivo de Auditoria, 10.2 - Gerenciamento de Recursos Humanos). Mesmo assim, a terceirização não libera a função de auditoria interna de sua responsabilidade pela conformidade com os Requisitos Temáticos. O chefe executivo de auditoria mantém a responsabilidade final de garantir a conformidade. Além disso, se o chefe executivo de auditoria determinar que os recursos de auditoria interna são insuficientes, ele deve informar o conselho sobre o impacto da insuficiência de recursos e como qualquer falta de recursos será tratada (Norma 8.2 - Recursos).

Desempenho, Documentação e Reporte

Ao aplicar os Requisitos Temáticos, os auditores internos também devem estar em conformidade com as Normas, conduzindo seu trabalho em alinhamento com o Domínio V: Execução dos Serviços de Auditoria Interna. As normas no Domínio V descrevem o planejamento de trabalhos (Princípio 13 - Planejar Trabalhos Efetivamente), a condução de trabalhos (Princípio 14 - Conduzir o Trabalho do Trabalho do Trabalho) e a comunicação dos resultados do trabalho (Princípio 15 - Comunicar os Resultados do Trabalho e Monitorar os Planos de Ação).

A cobertura do Requisito Temático pode ser documentada no plano de auditoria interna ou nos papéis de trabalho, com base no julgamento profissional dos auditores. Um ou mais trabalhos de auditoria interna podem abranger os requisitos. Além disso, nem todos os requisitos podem ser aplicáveis. As evidências de que a aplicabilidade do Requisito Temático foi avaliada devem ser guardadas, incluindo uma justificativa que explique quaisquer exclusões.

A ferramenta opcional no Anexo C pode ser usada como referência e para documentar o trabalho realizado pelos auditores internos.

Avaliação de Qualidade

As Normas exigem que o chefe executivo de auditoria desenvolva, implemente e mantenha um programa de avaliação e melhoria da qualidade que abranja todos os aspectos da função de auditoria interna (Norma 8.3 - Qualidade). Os resultados devem ser comunicados ao conselho e à alta administração. As comunicações devem reportar a conformidade da função de auditoria interna com as Normas e a concretização dos objetivos de desempenho.

A conformidade com os Requisitos Temáticos será avaliada nas avaliações de qualidade. Para se preparar para uma revisão de qualidade, os auditores internos podem usar a ferramenta fornecida no Anexo C.

Cibersegurança

A cibersegurança é um tema amplo, relacionado à maioria dos aspectos tecnológicos de qualquer organização. Além da tecnologia da informação, a cibersegurança geralmente faz parte dos processos de negócios, exigindo que os auditores internos avaliem os riscos relacionados à cibersegurança ao planejar, definir o escopo e realizar trabalhos de avaliação.

O National Institute of Standards and Technology (NIST), parte do Departamento de Comércio dos EUA, define a cibersegurança simplesmente como "a capacidade de proteger ou defender o uso do espaço cibernético contra ciberataques". O Requisito Temático de Cibersegurança concentra-se no perímetro externo, que as organizações protegem para reduzir os riscos de usuários não autorizados e ameaças cibernéticas maliciosas. A cibersegurança é um subconjunto da segurança da informação abrangente, que o NIST define como "a proteção de informações e sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer confidencialidade, integridade e disponibilidade".

Os requisitos do Requisito Temático de Cibersegurança incluem:

- Governança – Objetivos e estratégias de cibersegurança de linha de base claramente definidos, que apoiem as metas, políticas e procedimentos organizacionais.
- Gerenciamento de Riscos – Processos para identificar, analisar, gerenciar e monitorar ameaças cibernéticas, incluindo um processo para escalar riscos cibernéticos prontamente.
- Controles – Processos de controle estabelecidos pela gestão e avaliados periodicamente para reduzir o risco cibernético.

Considerações

Os auditores internos podem usar as seguintes considerações para ajudar na avaliação dos requisitos do Requisito Temático de Cibersegurança. Essas considerações, que fazem referência cruzada aos requisitos, são ilustrativas, mas não obrigatórias. Os auditores internos deveriam confiar em seu julgamento profissional ao determinar o que incluir em suas avaliações.

Considerações de Governança

Para avaliar como os processos de governança são aplicados aos objetivos de cibersegurança, os auditores internos podem analisar:

A. Plano estratégico e objetivos de cibersegurança formalizados e documentados, incluindo evidências de que o conselho analisa periodicamente (geralmente trimestralmente) as atualizações de cibersegurança fornecidas pelo chefe da função de segurança da informação, como o diretor de segurança da informação (CISO). As evidências podem incluir o reporte sobre:
   - Monitoramento da concretização dos objetivos estratégicos.
   - Necessidades orçamentárias para apoiar as metas e objetivos de cibersegurança.
   - Foco nos riscos e controles internos, incluindo o progresso de remediações.
   - Principais indicadores de desempenho (KPIs) para mensurar o sucesso.
   - Recursos humanos necessários para contratar, treinar e desenvolver a equipe de cibersegurança.

B. Políticas, procedimentos e outras documentações relevantes usadas para gerenciar processos de cibersegurança, incluindo:
   - Políticas revisadas e atualizadas pelo menos anualmente. Os riscos cibernéticos emergentes podem exigir que as revisões e atualizações ocorram com maior frequência.
   - Um processo para determinar se as políticas e os procedimentos são suficientes para apoiar as operações de cibersegurança.
   - Frameworks amplamente adotados (NIST, COBIT e outros) para fortalecer os processos de cibersegurança e os controles internos.

C. Papéis e responsabilidades que apoiem a concretização dos objetivos de cibersegurança, incluindo uma estrutura que garanta que a função de cibersegurança reporte a um nível na organização que tenha visibilidade suficiente para obter apoio organizacional.
   - Um processo para avaliar periodicamente o conhecimento, as competências e as habilidades da equipe que desempenha papéis de cibersegurança.

D. Evidências de envolvimento com os stakeholders relevantes (por exemplo, alta administração, operações, gerenciamento de riscos, recursos humanos, jurídico,

conformidade, fornecedores estratégicos e outros), incluindo comunicação sobre riscos cibernéticos existentes e emergentes e possíveis vulnerabilidades conhecidas. As evidências de comunicação podem incluir atas de reuniões, relatórios ou e-mails.

Considerações de Gerenciamento de Riscos

Para avaliar como os processos de gerenciamento de riscos são aplicados aos objetivos de cibersegurança, os auditores internos podem analisar:

A. Como a organização avalia e gerencia o risco de cibersegurança, incluindo como as ameaças e vulnerabilidades são:
   - Inicialmente identificadas e reportadas.
   - Analisadas, para avaliar o risco à concretização dos objetivos organizacionais.
   - Mitigadas, incluindo planos de ação para reduzir o risco a um nível aceitável.
   - Monitoradas, incluindo um plano para reporte contínuo até que as ameaças sejam totalmente resolvidas.

B. Como a organização obtém informações periódicas sobre o gerenciamento de riscos de cibersegurança de áreas funcionais, como tecnologia da informação, gerenciamento de riscos corporativos, recursos humanos, jurídico, conformidade, operações, contabilidade e finanças. Uma equipe multifuncional de cibersegurança ou um comitê de direcionamento de TI pode ser usado para obter informações.

C. Como a organização atribuiu a responsabilidade pelo gerenciamento de riscos de cibersegurança a um indivíduo ou equipe.
   - A(s) pessoa(s) responsável(is) deveria(m) comunicar periodicamente (trimestralmente, mensalmente ou conforme necessário) as atualizações contínuas dos riscos de cibersegurança em toda a organização e pode(m) incluir requisitos de recursos para estratégias de mitigação de riscos.

D. Os processos de escalonamento para riscos de cibersegurança, inclusive como o nível de ameaça ou risco é avaliado, atribuído e priorizado. A revisão pode incluir a identificação de:
   - Níveis de risco definidos pela organização – como alto, moderado e baixo – com explicações detalhadas de cada nível de risco e procedimentos de escalonamento para cada categoria de risco.
   - Lista de riscos de cibersegurança atualmente identificados e o status de mitigação de cada evento de risco.
   - Requisitos legais, regulatórios e de conformidade aplicáveis.
   - Impactos de riscos financeiros e não financeiros (por exemplo, reputação).

E. O processo de comunicação dos riscos de cibersegurança à gestão e aos funcionários, que inclui:

- Treinamento periódico (pelo menos anualmente) de cibersegurança para os funcionários, como campanhas de *phishing* simuladas e não anunciadas, para testar e acompanhar a conscientização organizacional.
- Atualizações sobre a remediação de problemas de cibersegurança existentes, com datas de conclusão previstas.
- Monitoramento de não conformidade, incluindo atualizações ao conselho e à alta administração.
- Reavaliação das ameaças quando o apetite e a tolerância a risco da organização mudarem.

F. Processos que a organização implementou com relação à resposta e recuperação de incidentes, que incluem:

- Um plano documentado revisado e atualizado conforme as operações da organização mudam ao longo do tempo. O plano deveria incluir:
  - Como os incidentes são detectados e reportados.
  - Como os incidentes são contidos, para evitar danos adicionais.
  - Como a organização se recuperará e reagirá para retomar as operações.
  - Como o incidente será analisado para identificar as lições aprendidas e como evitar eventos futuros semelhantes.
- Testes (exercício de mesa) periódicos (pelo menos anualmente) e comunicação dos resultados à alta administração e aos stakeholders relevantes. Planos de ação podem resultar dos testes.

Considerações de Processos de Controle

Para avaliar como os processos de controle são aplicados aos objetivos de cibersegurança, os auditores internos podem analisar:

A. A abordagem da gestão para criar um ambiente de controle interno de cibersegurança eficaz, incluindo:

- Avaliar e implementar os controles internos necessários para mitigar riscos elevados e proteger dados sensíveis, críticos, pessoais ou confidenciais, com base no processo de avaliação de riscos organizacionais.
- Determinação dos requisitos de recursos para manter os principais controles de cibersegurança.
- Considerar os controles baseados em fornecedores como parte do ambiente de controle, o que inclui a análise dos relatórios de controles da organização de serviços (SOC) dos fornecedores antes de iniciar o relacionamento comercial e durante todo o período do relacionamento.

- Testes periódicos para verificar se os controles de cibersegurança estão funcionando de forma a reduzir os riscos e apoiar a concretização dos objetivos de cibersegurança.
- Processo para corrigir deficiências de controle interno ou abordar constatações de avaliações realizadas pela função de auditoria interna ou por outros prestadores de avaliação (por exemplo, testes de penetração).

B. O processo de gestão de talentos da organização para recrutar e treinar profissionais de cibersegurança, incluindo como a organização identifica oportunidades de aumentar as capacidades dos profissionais de cibersegurança, para apoiar o conhecimento técnico e melhorar a conscientização organizacional sobre questões emergentes.
   - Exemplos incluem a participação em treinamentos, o envolvimento com grupos de compartilhamento de conhecimento e a educação profissional contínua, que inclui a obtenção de certificações relacionadas à cibernética.

C. O processo da gestão para identificar, priorizar, monitorar e reportar ameaças e vulnerabilidades emergentes de cibersegurança de forma contínua e focada nas operações diárias. A análise pode incluir o estabelecimento de processos para avaliar ameaças e vulnerabilidades relacionadas a tecnologias novas ou emergentes, como o uso de inteligência artificial.

D. Os processos e controles da gestão estabelecidos para gerenciar e proteger os ativos de TI durante todo o ciclo de vida, incluindo a seleção, uso, manutenção e desativação de hardware, software e serviços de fornecedores. Hardware inclui servidores, equipamentos de rede (como roteadores ou firewalls), desktops, laptops, telefones celulares, tablets e periféricos. Software inclui sistemas operacionais (como o Windows), programas de planejamento de recursos corporativos, aplicativos, programas antivírus e outros. As considerações sobre hardware e software podem incluir:
   - O uso de criptografia, software antivírus, gerenciamento de dispositivos móveis, requisitos de senhas complexas, rede privada virtual (VPN)/rede de confiança zero (ZTN) para autenticação e atualização periódica do firmware.
   - Um processo de gerenciamento de ativos que garanta que o hardware emitido pela empresa tenha uma configuração de segurança apropriada no momento da emissão e haja um descartado adequado quando os ativos forem aposentados.
   - Controles relacionados a bancos de dados, incluindo a limitação do acesso de usuários e administradores, avaliação do uso de criptografia, backup e teste de bancos de dados e presença de fortes controles de segurança de rede.
   - Como as ameaças ou vulnerabilidades de cibersegurança são consideradas no ciclo de vida de desenvolvimento do sistema (SDLC).
   - A abordagem usada pelo desenvolvimento, segurança e operações (DevSecOps) para garantir que o processo de desenvolvimento de software inclua a cibersegurança, para identificar vulnerabilidades de forma proativa.

E. Processos usados para fortalecer a cibersegurança, incluindo:
   - Configuração das definições de segurança para minimizar o risco de cibersegurança.
   - A administração de dispositivos móveis (incluindo o uso de e-mail e aplicativos) é configurada para reduzir os riscos de cibersegurança e ser gerenciada remotamente, se o dispositivo de um usuário for comprometido.
   - O uso de criptografia para dados "em repouso", como informações armazenadas em um disco rígido, ou dados "em trânsito", como a criptografia de e-mails.
   - Atualização de servidores ou software (como um sistema operacional) com as versões de segurança mais recentes.
   - Gerenciamento de acesso do usuário, como o uso de autenticação multifatorial (MFA) e IDs de usuário exclusivos, com senhas complexas que expiram periodicamente.
   - Controles de monitoramento em vigor para determinar se a disponibilidade e a utilização de recursos estão funcionando adequadamente, permitindo a revisão e a análise de possíveis problemas de cibersegurança que ameaçam o desempenho.
   - Integração da cibersegurança ao SDLC, para identificar e solucionar vulnerabilidades de cibersegurança antes que o software seja colocado em produção.

F. Controles relacionados à rede que protegem o perímetro da organização, incluindo como a organização utiliza:
   - Segmentação de rede.
   - Firewalls.
   - Controles de acesso do usuário.
   - Limitações para conexões externas e internas.
   - Controles relacionados à Internet das Coisas (IoT) para redes interconectadas.
   - Sistemas de detecção/prevenção de intrusão para evitar, detectar e se recuperar de ataques de cibersegurança.

G. Controles relacionados a controles de segurança de comunicação de *endpoint* aplicáveis a serviços como e-mail, navegadores de Internet, videoconferência, mensagens (Zoom, MS Teams e outros), redes sociais, nuvem e protocolos de compartilhamento de arquivos. Os controles podem incluir a restrição do uso de determinadas extensões de arquivo (como arquivos .exe) e autenticação multifatorial para compartilhamento de arquivos.

Anexo A. Exemplos de Aplicações Práticas

Os exemplos a seguir descrevem cenários em que o Requisito Temático de Cibersegurança seria aplicável:

Exemplo 1: A cibersegurança é identificada para um trabalho de auditoria interna incluído no plano de auditoria interna.

Quando a função de auditoria interna conclui seu processo de planejamento baseado em riscos e inclui um ou mais trabalhos sobre cibersegurança no plano de auditoria interna, o Requisito Temático é obrigatório ao conduzir esses trabalhos. A conformidade pode ser obtida com a inclusão dos requisitos em um ou mais trabalhos do plano de auditoria interna.

A cibersegurança é um tema amplo, e nem todos os requisitos do Requisito Temático podem ser aplicados em todos os trabalhos. Quando os auditores internos aplicam o julgamento profissional e determinam que um ou mais requisitos do Requisito Temático de Cibersegurança não são aplicáveis e, portanto, deveriam ser excluídos de um trabalho, os auditores internos devem documentar e guardar a justificativa para a exclusão desses requisitos. Por exemplo, a justificativa para a exclusão de alguns requisitos pode ser o fato de a função de auditoria interna realizar vários trabalhos de cibersegurança em uma base rotativa ou ter determinado que a importância do risco no trabalho é baixa.

Exemplo 2: Riscos de cibersegurança são identificados durante um trabalho de auditoria que não está focado na cibersegurança.

Os auditores internos podem identificar riscos à cibersegurança enquanto avaliam um processo não diretamente relacionado à cibersegurança. Por exemplo, os auditores internos podem estar avaliando o processo de contas a pagar em um trabalho não focado na cibersegurança e não identificar riscos de cibersegurança como parte do escopo ao planejar o trabalho. No entanto, depois de realizar o passo a passo inicial, os auditores internos determinam que esses riscos deveriam estar no escopo; por exemplo, eles identificam riscos de cibersegurança relacionados ao envio via Web de uma solicitação inicial de pedido de compra (Norma 13.2 - Avaliação de Riscos do Trabalho).

Uma vez identificados os riscos relevantes, os auditores internos devem analisar o Requisito Temático de Cibersegurança e determinar quais requisitos são aplicáveis. Neste exemplo, eles poderiam excluir o processo de governança da cibersegurança ou o processo de gerenciamento de riscos de cibersegurança. Eles devem documentar nos papéis de trabalho a justificativa para excluir os outros requisitos do Requisito Temático de Cibersegurança e guardar a documentação.

Exemplo 3: É solicitado um trabalho de cibersegurança que não foi originalmente incluído no plano de auditoria interna.

Os stakeholders, como o conselho, a gestão ou um regulador, podem solicitar que os auditores internos realizem avaliações de cibersegurança fora do plano de auditoria original. Por exemplo, quando as organizações são alvo de um ataque cibernético, o conselho pode solicitar um trabalho de auditoria interna para avaliar os controles de cibersegurança. O Requisito Temático é aplicável, os requisitos devem ser avaliados e quaisquer exclusões devem ser documentadas.

Anexo B. Mapeamento de Frameworks

A organização pode ter seus próprios esforços de cibersegurança, usando frameworks de gerenciamento de riscos e governança como COBIT ou NIST. Os auditores internos podem já ter desenvolvido programas de auditoria e procedimentos de teste com base nesses frameworks. Os auditores internos deveriam reconciliar com o Requisito Temático os seus testes de controle de cibersegurança pretendidos, para garantir a cobertura adequada. O gráfico abaixo mapeia o Requisito Temático de Cibersegurança para três frameworks comumente usados: NIST Cybersecurity Framework 2.0, COBIT 2019 e NIST 800-53. Esses frameworks foram mapeados, porque estão prontamente disponíveis sem custo.

Requisitos de Governança	Referências do Framework		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. A. São estabelecidos uma estratégia e objetivos formais de cibersegurança, atualizados periodicamente. As atualizações sobre a concretização dos objetivos de cibersegurança são periodicamente comunicadas e revisadas pelo conselho, incluindo recursos e considerações orçamentárias para apoiar a estratégia de cibersegurança.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Políticas e procedimentos relacionados à cibersegurança são estabelecidos e atualizados periodicamente, para fortalecer o ambiente de controle.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. São estabelecidos papéis e responsabilidades que apoiam os objetivos de cibersegurança e existe um processo para avaliar periodicamente o conhecimento, as habilidades e as capacidades dos indivíduos que desempenham esses papéis.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Os stakeholders relevantes são envolvidos, para discutir e agir quanto às vulnerabilidades existentes e às ameaças emergentes no ambiente de cibersegurança. Os stakeholders incluem a alta administração, as operações, o gerenciamento de riscos, os recursos humanos, o departamento jurídico, a conformidade, os fornecedores e outros.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Requisitos de Gerenciamento de Riscos	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Os processos de avaliação e gerenciamento de riscos da organização incluem a identificação, análise, mitigação e monitoramento das ameaças à cibersegurança e seu efeito sobre a concretização dos objetivos estratégicos.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. O gerenciamento de riscos de cibersegurança é realizado em toda a organização e pode incluir as seguintes áreas: tecnologia da informação, gerenciamento de riscos corporativos, recursos humanos, jurídico, conformidade, operações, cadeia de suprimentos, contabilidade, finanças e outras.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. São estabelecidas prestação de contas e responsabilidades pelo gerenciamento de riscos de cibersegurança. Um indivíduo ou equipe é identificado para monitorar e reportar periodicamente como os riscos de cibersegurança estão sendo gerenciados, incluindo os recursos necessários para mitigar os riscos e identificar ameaças emergentes à cibersegurança.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Um processo é estabelecido para escalar rapidamente qualquer risco de cibersegurança (emergente ou previamente identificado) que atinja um nível inaceitável de acordo com as diretrizes de gerenciamento de riscos estabelecidas pela organização ou com os requisitos legais e regulatórios aplicáveis. Os impactos financeiros e não financeiros do risco de cibersegurança deveriam ser considerados.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Foi estabelecido um processo para conscientizar a gestão e os funcionários sobre os riscos de cibersegurança e para a gestão analisar periodicamente problemas, lacunas, deficiências ou falhas de controle com relatórios e correções tempestivos.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. A organização implementou um processo de resposta e recuperação após incidentes de cibersegurança que inclui detecção, contenção, recuperação e análise pós-incidente. O processo de resposta e recuperação após incidentes é testado periodicamente.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Requisitos de Processos de Controle	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Um processo é estabelecido para garantir que controles internos e controles de fornecedores estejam em vigor, para proteger a confidencialidade, a integridade e a disponibilidade dos sistemas e dados da organização. Avaliações são realizadas periodicamente para determinar se os controles estão funcionando de forma a promover a concretização dos objetivos de cibersegurança da organização e a resolução imediata de problemas.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. É estabelecido um processo de gestão de talentos que inclui treinamento para desenvolver e manter as competências técnicas relacionadas às operações de cibersegurança. O processo é revisado periodicamente.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. É estabelecido um processo para monitorar e reportar continuamente as ameaças e vulnerabilidades emergentes de cibersegurança e para identificar, priorizar e implementar oportunidades de melhoria para as operações de cibersegurança.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. A cibersegurança está incluída no gerenciamento do ciclo de vida (seleção, uso, manutenção e desativação) de todos os ativos de TI, inclusive hardware, software e serviços de fornecedores.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. São estabelecidos processos para fortalecer a cibersegurança, incluindo configuração, administração de dispositivos do usuário final, criptografia, aplicação de patches, gerenciamento de acesso do usuário e monitoramento da disponibilidade e do desempenho. Considerações de cibersegurança são incluídas no desenvolvimento de software (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. São estabelecidos controles relacionados à rede, como controles de acesso à rede e segmentação; uso e posicionamento de firewalls; conexões limitadas de e para redes externas; rede privada virtual (VPN)/acesso à rede de confiança zero (ZTNA); controles de rede da Internet das Coisas (IoT); e sistemas de detecção/prevenção de intrusão (IDS e IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. São estabelecidos controles de segurança de comunicação de *endpoint* para serviços como e-mail, navegadores de Internet, videoconferência, mensagens, redes sociais, nuvem e protocolos de compartilhamento de arquivos	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Anexo C. Ferramenta de Documentação Opcional

Espera-se que os auditores internos exerçam julgamento profissional ao determinar a aplicabilidade dos requisitos com base na avaliação de riscos e documentem adequadamente as exclusões de determinados requisitos. O Requisito Temático pode ser documentado no plano de auditoria interna ou nos papéis de trabalho, com base no julgamento profissional do auditor. Um ou mais trabalhos de auditoria interna podem abordar os requisitos. Além disso, nem todos os requisitos podem ser aplicáveis. O formulário para impressão abaixo oferece uma opção para documentar a conformidade com o Requisito Temático de Cibersegurança, mas seu uso não é obrigatório.

Cibersegurança – Governança

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
A. A. São estabelecidos uma estratégia e objetivos formais de cibersegurança, atualizados periodicamente. As atualizações sobre a concretização dos objetivos de cibersegurança são periodicamente comunicadas e revisadas pelo conselho, incluindo recursos e considerações orçamentárias para apoiar a estratégia de cibersegurança.		
B. Políticas e procedimentos relacionados à cibersegurança são estabelecidos e atualizados periodicamente, para fortalecer o ambiente de controle.		
C. São estabelecidos papéis e responsabilidades que apoiam os objetivos de cibersegurança e existe um processo para avaliar periodicamente o conhecimento, as habilidades e as capacidades dos indivíduos que desempenham esses papéis.		

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
D. Os stakeholders relevantes são envolvidos, para discutir e agir quanto às vulnerabilidades existentes e às ameaças emergentes no ambiente de cibersegurança. Os stakeholders incluem a alta administração, as operações, o gerenciamento de riscos, os recursos humanos, o departamento jurídico, a conformidade, os fornecedores e outros.		

Cibersegurança – Gerenciamento de riscos

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
A. Os processos de avaliação e gerenciamento de riscos da organização incluem a identificação, análise, mitigação e monitoramento das ameaças à cibersegurança e seu efeito sobre a concretização dos objetivos estratégicos.		
B. O gerenciamento de riscos de cibersegurança é realizado em toda a organização e pode incluir as seguintes áreas: tecnologia da informação, gerenciamento de riscos corporativos, recursos humanos, jurídico, conformidade, operações, cadeia de suprimentos, contabilidade, finanças e outras.		

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
C. São estabelecidas prestação de contas e responsabilidades pelo gerenciamento de riscos de cibersegurança. Um indivíduo ou equipe é identificado para monitorar e reportar periodicamente como os riscos de cibersegurança estão sendo gerenciados, incluindo os recursos necessários para mitigar os riscos e identificar ameaças emergentes à cibersegurança.		
D. Um processo é estabelecido para escalar rapidamente qualquer risco de cibersegurança (emergente ou previamente identificado) que atinja um nível inaceitável de acordo com as diretrizes de gerenciamento de riscos estabelecidas pela organização ou com os requisitos legais e regulatórios aplicáveis. Os impactos financeiros e não financeiros do risco de cibersegurança deveriam ser considerados.		
E. Foi estabelecido um processo para conscientizar a gestão e os funcionários sobre os riscos de cibersegurança e para a gestão analisar periodicamente problemas, lacunas, deficiências ou falhas de controle com relatórios e correções tempestivos.		
F. A organização implementou um processo de resposta e recuperação após incidentes de cibersegurança que inclui detecção, contenção, recuperação e análise pós-incidente. O processo de resposta e recuperação após incidentes é testado periodicamente.		

Cibersegurança – Processos de Controle

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
A. Um processo é estabelecido para garantir que controles internos e controles de fornecedores estejam em vigor, para proteger a confidencialidade, a integridade e a disponibilidade dos sistemas e dados da organização. Avaliações são realizadas periodicamente para determinar se os controles estão funcionando de forma a promover a concretização dos objetivos de cibersegurança da organização e a resolução imediata de problemas.		
B. É estabelecido um processo de gestão de talentos que inclui treinamento para desenvolver e manter as competências técnicas relacionadas às operações de cibersegurança. O processo é revisado periodicamente.		
C. É estabelecido um processo para monitorar e reportar continuamente as ameaças e vulnerabilidades emergentes de cibersegurança e para identificar, priorizar e implementar oportunidades de melhoria para as operações de cibersegurança.		
D. A cibersegurança está incluída no gerenciamento do ciclo de vida (seleção, uso, manutenção e desativação) de todos os ativos de TI, inclusive hardware, software e serviços de fornecedores.		

Requisito	Cobertura executada ou justificativa para exclusão	Referência de documentação
E. São estabelecidos processos para fortalecer a cibersegurança, incluindo configuração, administração de dispositivos do usuário final, criptografia, aplicação de patches, gerenciamento de acesso do usuário e monitoramento da disponibilidade e do desempenho. Considerações de cibersegurança são incluídas no desenvolvimento de software (DevSecOps).		
F. São estabelecidos controles relacionados à rede, como controles de acesso à rede e segmentação; uso e posicionamento de firewalls; conexões limitadas de e para redes externas; rede privada virtual (VPN)/acesso à rede de confiança zero (ZTNA); controles de rede da Internet das Coisas (IoT); e sistemas de detecção/prevenção de intrusão (IDS e IPS).		
G. São estabelecidos controles de segurança de comunicação de *endpoint* para serviços como e-mail, navegadores de Internet, videoconferência, mensagens, redes sociais, nuvem e protocolos de compartilhamento de arquivos		

Sobre o Instituto de Auditores Internos

O Institute of Internal Auditors (The IIA) é uma associação profissional internacional que atende a mais de 255.000 membros globais e concedeu mais de 200.000 certificações *Certified Internal Auditor*® (CIA®) em todo o mundo. Fundado em 1941, o The IIA é reconhecido no mundo todo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, acesse www.theiia.org.

Isenção de Responsabilidade

O IIA publica este documento para fins informativos e educacionais. Este material não tem a intenção de fornecer respostas definitivas para circunstâncias individuais específicas e, portanto, deve ser usado apenas como um guia. O IIA recomenda a busca de assessoria especializada independente relacionada diretamente a qualquer situação específica. O IIA não se responsabiliza por casos em que qualquer pessoa confie exclusivamente neste material.

Copyright

Fevereiro de 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101