Requisito Tópico de Cibersegurança

O que são requisitos tópicos?

Os Requisitos Temáticos são um componente essencial da Estrutura Internacional de Práticas Profissionais® , que também inclui as Normas Globais de Auditoria Interna™ e a Orientação Global. O Institute of Internal Auditors, como definidor de padrões para a profissão de auditoria interna, exige esses Requisitos Temáticos obrigatórios como um suplemento às Normas Globais de Auditoria Interna, que servem como autoridade para as práticas exigidas descritas e com referências cruzadas nos Requisitos Temáticos.

Os Requisitos Temáticos fornecem uma estrutura para tópicos globais frequentemente auditados que são tipicamente de risco mais elevado e de natureza generalizada. Embora as Normas se apliquem a todos os serviços de auditoria interna prestados, um Requisito Temático deve ser considerado como um requisito obrigatório adicional a ser seguido quando esse assunto é o foco de um trabalho de auditoria interna.

Os Requisitos Temáticos devem ser aplicados ao nível da entidade ou da organização a tópicos que tenham impacto em toda a organização. Os auditores internos devem estar familiarizados com os Requisitos Temáticos e estar preparados para os aplicar quando o tópico for incluído nos seus planos de auditoria anuais ou se esse tópico específico for o foco de um trabalho de auditoria interna. Os elementos do requisito temático devem ser avaliados aquando da definição do âmbito do trabalho. As provas de que a avaliação e o tratamento do tema ocorreram devem ser documentadas e conservadas. Os trabalhos que incluam qualquer aspeto do tópico devem avaliar os requisitos relevantes para o trabalho ou documentar a razão pela qual os requisitos específicos não são aplicáveis. No Apêndice B é fornecida uma ferramenta para ajudar os auditores internos a explicar a fundamentação da inclusão ou exclusão de requisitos.

Por que razão são necessários requisitos tópicos?

A aplicação dos Requisitos Temáticos destina-se a reforçar a relevância contínua de uma função de auditoria interna para o panorama de risco global em evolução e a aumentar o valor dos serviços de auditoria interna em todas as indústrias e sectores. A conformidade com os Requisitos Temáticos ajudará os auditores internos a aumentar a qualidade e a consistência dos trabalhos.

Os Requisitos Temáticos estão estruturados de forma a fornecer orientações para a prestação de serviços de auditoria interna em três áreas: governação, gestão do risco e processos de controlo. Cada área inclui:

- Requisitos, que são obrigatórios e abrangem objectivos organizacionais essenciais.
- Considerações, que não são obrigatórias, mas servem como melhores práticas para avaliar a conceção e a implementação dos objectivos organizacionais. As considerações, fornecidas no Apêndice A, devem ser utilizadas simplesmente como exemplos para validar os requisitos.

A conformidade com os requisitos temáticos será avaliada nas avaliações de qualidade. Para demonstrar a conformidade na preparação de uma análise da qualidade, os auditores internos devem utilizar a ferramenta fornecida no Apêndice B para indicar a conformidade com cada requisito ou para explicar porque é que a conformidade não foi alcançada.

Requisito Tópico de Cibersegurança

Avaliação e apreciação da eficácia dos processos de governação, gestão de riscos e controlo da cibersegurança

A cibersegurança protege os activos de informação de uma organização contra utilizadores não autorizados, perturbação, alteração ou destruição, e reforça o ambiente de controlo global para reduzir o risco. Os ciberataques podem levar a impactos directos e indirectos que são frequentemente significativos, uma vez que os computadores, redes, programas, dados e informações sensíveis são componentes críticos da maioria das organizações. Uma vez que as organizações dependem fortemente dos recursos das tecnologias da informação, a definição clara de um plano de cibersegurança, objectivos, riscos inerentes e controlos eficazes deve ser uma prioridade para a gestão.

Este requisito temático fornece uma abordagem coerente e abrangente para avaliar a conceção e a implementação de processos de governação, gestão de riscos e controlo da cibersegurança.

GOVERNANÇA: Avaliação e apreciação da governação da cibersegurança

Requisitos:

Ao realizar um trabalho de auditoria interna que inclua objectivos de cibersegurança no seu âmbito, os auditores internos devem avaliar se os processos de governação da organização abordam adequadamente a cibersegurança. Os auditores internos devem avaliar se:

A. As políticas e os procedimentos relacionados com os processos de gestão dos riscos de cibersegurança são estabelecidos e periodicamente actualizados, incluindo a promoção de práticas que reforçam o ambiente de controlo com base em quadros amplamente adoptados (NIST, COBIT e outros).

B. As funções e responsabilidades que apoiam os objectivos de cibersegurança da organização estão claramente definidas e essas funções são preenchidas por indivíduos com os conhecimentos, competências e capacidades necessários.

C. As actualizações dos objectivos, estratégias, riscos e controlos de atenuação da cibersegurança são comunicadas periodicamente ao conselho de administração.

D. As partes interessadas relevantes (por exemplo, liderança, operações, fornecedores estratégicos e outros) são envolvidas para discutir a melhor forma de estabelecer e melhorar os processos de gestão dos riscos de cibersegurança.

E. Os recursos necessários (tais como liderança, financiamento, talento, hardware, software e formação) para executar eficazmente os processos de gestão do risco de cibersegurança são comunicados ao conselho de administração.

GESTÃO DO RISCO: Avaliação e apreciação da gestão do risco de cibersegurança

Requisitos:

Ao realizar um trabalho de auditoria interna que inclua objectivos de cibersegurança no seu âmbito, os auditores internos devem avaliar se os processos de gestão do risco da organização abordam adequadamente a cibersegurança. Os auditores internos devem avaliar se:

A. É estabelecido um processo de gestão do risco a nível da organização que inclui a identificação, análise e gestão dos riscos relacionados com as tecnologias e a segurança da informação, com especial incidência nos riscos de cibersegurança e na forma como esses riscos podem afetar a capacidade de atingir os objectivos organizacionais.

B. Os processos de gestão do risco de cibersegurança são conduzidos por uma equipa multifuncional que inclui a liderança das tecnologias de informação, a gestão do risco em toda a organização, o departamento jurídico, a conformidade, outras entidades de gestão (operações, contabilidade, finanças e outras) e envolve partes externas (vendedores, prestadores de serviços subcontratados, fornecedores, clientes e outros), conforme aplicável.

C. As políticas e procedimentos de gestão do risco de cibersegurança foram estabelecidos e são periodicamente actualizados, incluindo a promoção de práticas que reforçam os processos de gestão do risco de cibersegurança com base em quadros de gestão do risco amplamente adoptados, orientações autorizadas ou outras melhores práticas.

D. A responsabilidade pela gestão dos riscos de cibersegurança está definida e foi identificado um indivíduo ou uma equipa que monitoriza e comunica periodicamente a forma como os riscos de cibersegurança estão a ser geridos, incluindo os requisitos de recursos para atenuar os riscos e a identificação de riscos emergentes de cibersegurança que não tinham sido identificados anteriormente.

E. É estabelecido um processo para escalar rapidamente quaisquer riscos de cibersegurança (emergentes ou previamente identificados) que atinjam níveis inaceitáveis com base nas directrizes de gestão de riscos estabelecidas pela organização ou para cumprir os requisitos legais e/ou regulamentares aplicáveis.

F. A gestão do risco de cibersegurança inclui a coordenação entre a segurança da informação, o departamento jurídico, a conformidade e outras entidades de gestão para identificar e cumprir todas as obrigações legais e contratuais, tais como leis e regulamentos. O estado de conformidade e não conformidade com os requisitos aplicáveis é comunicado periodicamente na organização.

G. É estabelecido um processo para identificar e gerir os riscos de cibersegurança relacionados com terceiros. Os vendedores, fornecedores e outros prestadores de processos e/ou serviços externalizados são contratualmente obrigados a implementar controlos eficazes de cibersegurança que protejam adequadamente a confidencialidade, a integridade e a disponibilidade dos sistemas e dados da organização a que terceiros têm acesso.

H. As políticas e os processos relacionados com a classificação, a retenção, a destruição e a cifragem dos dados são concebidos de forma adequada e aplicados eficazmente para proporcionar uma abordagem sistemática que garanta o registo completo e exato dos dados e proteja a confidencialidade e a privacidade das informações sensíveis.

I. É estabelecido um processo de comunicação dos riscos operacionais de cibersegurança para garantir a sensibilização da direção e dos trabalhadores. Quaisquer questões, lacunas, deficiências ou falhas de controlo são comunicadas ao conselho de administração e à direção, e o estado da correção é acompanhado de perto e comunicado. A não conformidade com as políticas de cibersegurança é identificada, investigada, comunicada e corrigida atempadamente.

CONTROLES: Avaliação e apreciação dos processos de controlo da cibersegurança

Requisitos:

Ao realizar um trabalho de auditoria interna que inclua objectivos de cibersegurança no seu âmbito, os auditores internos devem avaliar se os processos de controlo da organização abordam adequadamente a cibersegurança. Os auditores internos devem avaliar se a organização:

A. Dá prioridade aos controlos de cibersegurança e assegura que o orçamento e os recursos correspondentes (como pessoal, software, ferramentas e outros) são atribuídos para maximizar os benefícios esperados.

B. Assegura que os controlos de cibersegurança funcionam de forma a promover a realização dos objectivos organizacionais em matéria de cibersegurança e a resolução atempada dos problemas.

C. Fornece formação suficiente ao pessoal responsável pelas operações de cibersegurança.

D. Desenvolveu políticas e procedimentos suficientes para gerir todos os aspectos das operações de cibersegurança e controlos conexos.

E. Garante que a administração dispõe dos recursos necessários para se manter informada sobre as questões de cibersegurança emergentes das novas tecnologias, identificar oportunidades para melhorar as operações e compreender como os esforços de cibersegurança podem ser melhor utilizados para influenciar metas e objectivos organizacionais mais amplos.

F. Integra adequadamente a cibersegurança no ciclo de vida de desenvolvimento de sistemas para aplicações comerciais, incluindo software e aplicações adquiridas ou desenvolvidas à medida.

G. Incluiu a cibersegurança na gestão do hardware (como computadores portáteis, computadores de secretária, dispositivos móveis).

H. Implementou controlos eficazes relativamente ao suporte de hardware de produção, tais como a configuração, a aplicação de patches, o suporte da gestão do acesso dos utilizadores e a monitorização da disponibilidade e do desempenho. A organização avaliou a adequação da conceção e a eficácia operacional destes controlos.

I. Optimiza os controlos relacionados com a rede no que se refere à segmentação da rede, à utilização e colocação de firewalls, às ligações limitadas a redes e/ou sistemas externos e à utilização de tecnologias preventivas e de deteção, como os sistemas de deteção/prevenção de intrusões.

J. Implementou controlos eficazes em torno dos serviços comuns de comunicação em ambiente de trabalho, tais como correio eletrónico, navegadores de Internet, videoconferência, mensagens e protocolos de partilha de ficheiros.

K. Implementou controlos adequados da prestação de serviços para garantir que as seguintes áreas estão integradas na monitorização da cibersegurança: gestão de alterações, serviço/balcão de apoio e administração de dispositivos do utilizador final.

L. Implementou controlos de segurança física adequados para proteger os centros de informação de alto risco (tais como centros de dados, centros de operações de rede e centros de operações de segurança) contra ataques.

M. Implementou controlos de resposta a incidentes e de recuperação.

Normas relacionadas:

3.1 Competências
4.2 Cuidados profissionais devidos
9.1 Compreender a governação, a gestão do risco e os processos de controlo
9.4 Plano de auditoria interna
12.3 Supervisionar e melhorar o desempenho do compromisso
13.1 Comunicação do envolvimento
13.2 Avaliação dos riscos do compromisso
13.3 Objectivos e âmbito do compromisso
13.4 Critérios de avaliação
13.5 Recursos de envolvimento
13.6 Programa de trabalho
14.1 Recolha de informações para análise e avaliação
14.2 Análises e potenciais resultados do envolvimento
14.3 Avaliação dos resultados
14.4 Recomendações e planos de ação
14.5 Conclusões do envolvimento
14.6 Documentação do compromisso
15.1 Comunicação final do compromisso
15.2 Confirmação da implementação de recomendações ou planos de ação

Guias Globais de Auditoria Tecnológica (GTAGs) relacionados:

Avaliação do risco de cibersegurança: o modelo das três linhas
Auditoria de aplicações empresariais
Auditoria da resposta e recuperação de incidentes cibernéticos
Auditoria das operações de cibersegurança: Prevenção e deteção
Auditoria da gestão de identidades e acessos
Auditoria da governação das TI
Auditoria da computação móvel
Auditoria da gestão das redes e das comunicações

Apêndice A. Considerações

Considerações sobre cada requisito de governação:

Para avaliar a forma como os processos essenciais de governação são aplicados aos objectivos de cibersegurança, os auditores internos podem analisar

A. Políticas, procedimentos e outra documentação relevante utilizada pela organização para gerir as responsabilidades diárias em matéria de cibersegurança, incluindo:
   1. Documentação clara, concisa, coerente e actualizada periodicamente, de preferência à medida que são identificados os novos riscos de cibersegurança e, pelo menos, anualmente.
   2. Procedimentos relacionados com a identificação, análise, resolução e comunicação de violações ou outras perdas de dados sensíveis.
   3. Documentação sobre a forma como a direção garante que as políticas e os procedimentos são suficientes para apoiar as operações de cibersegurança.

B. Funções e responsabilidades criadas pelo conselho de administração para apoiar a concretização da estratégia de cibersegurança, incluindo uma estrutura de reporte que garanta que a cibersegurança é reportada a um nível da organização com visibilidade suficiente para obter apoio organizacional.

C. Materiais apresentados ao conselho de administração sobre a estratégia, os objectivos, os riscos e os controlos da cibersegurança, incluindo a análise da questão:
   1. A frequência da comunicação é adequada, idealmente trimestral e apresentada pelo responsável pela função de segurança da informação, por exemplo, um diretor de sistemas de informação.
   2. As informações apresentadas são claras, concisas e coerentes; os riscos e os controlos são comunicados de forma a serem facilmente compreendidos pelo conselho de administração.
   3. São incluídos indicadores-chave de desempenho ou outras métricas/estatísticas importantes em matéria de cibersegurança.
   4. Se for caso disso, a direção recebe e implementa os contributos do conselho de administração, comunicando-lhe as actualizações do estado das alterações.

D. Evidência das comunicações da direção relacionadas com a cibersegurança com as partes interessadas relevantes (por exemplo, liderança, operações, fornecedores estratégicos e outros), incluindo o facto de a informação comunicada ser clara, concisa, consistente e adaptada à audiência das partes interessadas:
   1. Empregados.
   2. Vendedores, fornecedores, prestadores de serviços subcontratados e terceiros.
   3. Clientes.
   4. Parceiros estratégicos.

E. A análise e a comunicação das necessidades de recursos pela direção, incluindo:
   1. Compreender como são identificadas as lacunas e quais as principais métricas utilizadas para antecipar alterações nos requisitos.
   2. Como é que a gestão trabalha com os recursos humanos para analisar as necessidades de talentos em matéria de cibersegurança.
   3. Como é que a gestão analisa os inventários actuais de hardware e software e determina se é necessário um investimento adicional para apoiar as iniciativas de cibersegurança.
   4. Se os auditores internos analisam a forma como a direção estabelece e actualiza os materiais de formação em matéria de cibersegurança e identifica as lacunas, incluindo a garantia de que a formação abrange os objectivos, riscos e controlos emergentes em matéria de cibersegurança.

Considerações sobre cada requisito de gestão de riscos:

Para avaliar os aspectos necessários da gestão do risco de cibersegurança, os auditores internos podem analisar

A. Como é que a gestão identifica inicialmente os riscos de cibersegurança, incluindo:
    1. Compreender que pessoal é responsável pelas ameaças diárias que a organização enfrenta e pelos riscos emergentes com a comunidade de segurança da informação.
        a. Determi ne se esses indivíduos têm a experiência profissional e a formação necessárias para reconhecer e transmitir eficazmente as ameaças à equipa de gestão de riscos mais vasta .
    2. Identificar as aplicações de software ou os fornecedores em que a direção confia para identificar os riscos de cibersegurança.
    3. Documentação relacionada com o processo de gestão do risco de cibersegurança, incluindo
        a. Ata da reunião.
        b. Pontos de ação.
        c. Listas de participantes ou membros da equipa.
        d. Investigação pós-incidente/análise da causa principal.

B. A forma como a direção identifica ou nomeia os membros da equipa de gestão do risco e a respectiva fundamentação ou qualificações utilizadas para avaliar a qualidade de membro. Analisar as provas da participação periódica em debates sobre o risco de cibersegurança com as partes externas relevantes.

C. O processo que a organização utiliza para estabelecer e atualizar periodicamente políticas e procedimentos relacionados com a gestão do risco de cibersegurança, que pode incluir:
    1. Uma revisão e aprovação anual das políticas e procedimentos.
    2. Compreensão da forma como a organização assegura o cumprimento das suas políticas e procedimentos de gestão do risco e da forma como o pessoal recebe formação sobre a execução das políticas e procedimentos.
        a. Compreensão dos quadros ou orientações oficiais que a direção utiliza para gerir os riscos de cibersegurança (NIST, COBIT e outros) e da forma como a organização confirma a adesão ao(s) quadro(s) escolhido(s).

D. O(s) indivíduo(s) responsável(eis) pela execução da gestão dos riscos de cibersegurança, incluindo a garantia de que a sua formação profissional, experiência, qualificações e credenciais são adequadas para gerir os riscos e ameaças à segurança da informação. Verificar se o indivíduo responsável está posicionado a um nível dentro da organização para dar visibilidade aos riscos de cibersegurança e comunicar esses riscos de forma eficaz.

E. Os processos de escalonamento que a organização utiliza para comunicar riscos de cibersegurança, incluindo a forma como o nível de ameaça ou risco é avaliado, atribuído e priorizado. Verificar se a organização definiu níveis de risco, como alto, moderado, baixo, incluindo uma explicação detalhada para cada nível de risco e procedimentos de escalonamento para cada categoria de risco. Rever a listagem dos actuais riscos de cibersegurança identificados e o estado de atenuação de cada evento.

F. O processo que a organização utiliza para garantir a conformidade com todos os regulamentos de cibersegurança aplicáveis, incluindo:
    1. Como os regulamentos propostos ou recentemente adoptados afectam a organização.
    2. Se existe um inventário dos regulamentos aplicáveis que é monitorizado, atualizado e comunicado periodicamente para garantir a sensibilização da organização.
        a. Relativamente a qualquer incumprimento, verificar se a direção tem conhecimento dos riscos associados, nomeadamente através de relatórios periódicos.

G. O processo da organização para gerir os riscos de cibersegurança de terceiros. Verificar se os controlos de cibersegurança do fornecedor são revistos antes do início de uma relação comercial e se os contratos incluem o

direito a revisões periódicas ao longo da relação. Incluir a obtenção e análise do relatório de controlos da organização de serviços do terceiro e verificar se a organização documentou a sua revisão do relatório SOC, que deve incluir a garantia de que as considerações de controlo do utilizador foram implementadas. Compreender a abordagem da administração para determinar se os terceiros têm um ambiente de controlo adequado que seja proporcional aos controlos da organização.

   a. Se forem detectadas deficiências de controlo de terceiros, compreender o processo que a gestão utiliza para se assegurar de que as deficiências não comprometem a cibersegurança relacionada com as operações, ou compreender como é que a organização comunica que são necessárias alterações para manter a relação com o fornecedor aplicável ou que deve ser encontrado um fornecedor de substituição.

H. As políticas e processos que a organização estabeleceu relacionados com:
   1. Classificação dos dados.
   2. Retenção de dados.
   3. Destruição de dados.
   4. Encriptação.
   5. Gestão do acesso/identidade.
   6. Quem prepara, revê e actualiza a documentação, que idealmente deve incluir pessoal jurídico e de conformidade para garantir a conformidade com os regulamentos aplicáveis.
   7. A forma como a organização efectua a classificação dos dados para garantir que os dados confidenciais e privados foram identificados e têm o nível de proteção adequado, como a limitação do acesso dos utilizadores.
   8. Como é que a organização analisa periodicamente o processo utilizado para classificar os dados e se o processo continua a apoiar os objectivos de cibersegurança da organização e a cumprir as políticas da organização e os regulamentos aplicáveis.

I. O processo de comunicação dos riscos operacionais de cibersegurança à direção e aos trabalhadores. Idealmente, essa comunicação deve ser incluída na formação periódica sobre cibersegurança (pelo menos anualmente). Compreender o processo de comunicação, por parte da direção, das actualizações relativas à resolução dos problemas de cibersegurança, bem como das datas previstas para a sua conclusão. Verificar se a não conformidade é acompanhada de perto e se são fornecidas actualizações ao conselho de administração e à direção.

Considerações sobre cada requisito do processo de controlo:

Para avaliar os aspectos necessários dos controlos de cibersegurança, os auditores internos podem analisar

A. O processo da direção para determinar a forma de utilizar os recursos orçamentados para apoiar o ambiente de controlo da cibersegurança, que deve incluir um planeamento estratégico anual para garantir que está disponível um nível adequado de recursos organizacionais para cumprir os objectivos de cibersegurança. Deverão ser analisados os resultados formais e documentados do planeamento anual e do acompanhamento periódico da gestão dos recursos.

B. Processo da direção para avaliar periodicamente se os controlos de cibersegurança estão a funcionar de forma a promover a realização dos objectivos de cibersegurança da organização. Verificar se a direção monitoriza a eficácia dos controlos e avalia se os controlos existentes foram concebidos de forma adequada ou se são necessários novos controlos. Em muitas organizações, a função de auditoria interna desempenha um papel significativo neste processo, garantindo a conceção dos controlos e a eficácia do seu funcionamento através de testes periódicos (trimestrais, anuais). Verificar os processos da gestão para corrigir as deficiências de controlo ou abordar as conclusões das avaliações realizadas pela função de auditoria interna ou por outros prestadores de garantias (por exemplo, testes de penetração).

C. O processo da direção para avaliar as necessidades de formação do pessoal de cibersegurança da organização e a forma como os recursos são atribuídos para ministrar a formação adequada e garantir que as ameaças emergentes à cibersegurança são compreendidas e geridas. Compreender de que forma a direção garante que os funcionários têm formação suficiente em cibersegurança, que pode incluir eventos de formação ao vivo, instruções gravadas ou a conclusão de módulos de formação.

D. O processo da organização para criar e atualizar políticas e procedimentos de cibersegurança e a forma como a direção avalia se essas políticas e procedimentos são adequados. Compreender de que forma o pessoal responsável pelas operações e controlos de cibersegurança recebe formação sobre o cumprimento das políticas e procedimentos e como é avaliada a sua conformidade interna.

E. O processo da organização para formar adequadamente a equipa de gestão responsável pelas operações e controlos de cibersegurança para reconhecer as tendências emergentes e fornecer às suas equipas e à organização uma liderança estratégica. Compreender de que forma a organização identifica oportunidades para aumentar as capacidades da direção para apoiar a sensibilização para questões emergentes, tais como a participação em formação e educação profissional contínua.

F. A forma como a organização aborda a cibersegurança no seu ciclo de vida de desenvolvimento de sistemas, incluindo os seguintes aspectos de controlo
    1. Planeamento: A cibersegurança foi identificada como um componente essencial na avaliação dos riscos e na análise de potenciais vulnerabilidades. O âmbito e os objectivos da implementação do software devem ser incluídos à medida que a organização avalia os controlos de cibersegurança durante a fase de planeamento.
    2. Recolha de requisitos: Os requisitos de cibersegurança são uma componente da definição dos requisitos funcionais, que também devem incluir o cumprimento de todos os requisitos legais e regulamentares aplicáveis.
    3. Conceção: As considerações relativas à cibersegurança são incluídas como parte integrante dos requisitos de processamento pormenorizados. Os controlos devem ser identificados em todos os aspectos da conceção, à medida que a organização define mais formalmente as necessidades da conceção da arquitetura do sistema (tais como plataformas, interfaces de utilizador, bases de dados e outros).
    4. Desenvolvimento: A organização estabeleceu um ambiente seguro e definiu formalmente um processo de desenvolvimento que minimiza as vulnerabilidades cibernéticas (por exemplo, acesso limitado do utilizador ao código de desenvolvimento, separação adequada do ambiente de produção, utilização de ferramentas aprovadas, existência de pistas de auditoria para acompanhar as actividades de desenvolvimento, requisitos específicos de cibersegurança para software desenvolvido pelo fornecedor, etc.).
    5. Testes: A organização inclui a revisão e a avaliação da cibersegurança durante a fase de testes (por exemplo, testes automatizados, testes de penetração e avaliação de vulnerabilidades). A organização deve ser capaz de ser rapidamente alertada para quaisquer vulnerabilidades cibernéticas identificadas através de testes e de as resolver, o que inclui uma descrição pormenorizada da vulnerabilidade e das alterações ao código ou dos controlos de atenuação estabelecidos em resposta.
    6. Implementação: À medida que o novo software é colocado em produção, a organização deve monitorizar cuidadosamente as potenciais ameaças à cibersegurança, incluindo a garantia de que os utilizadores finais receberam formação para utilizar o software de forma a minimizar os riscos de cibersegurança. A organização deve garantir que os eventos e erros são registados e analisados em relação a potenciais eventos de cibersegurança.
    7. Manutenção: A organização deve garantir que todas as versões de software relacionadas com a segurança são aplicadas atempadamente e deve ter uma comunicação aberta com os fornecedores de software para garantir que os riscos e ameaças emergentes são devidamente controlados e que os utilizadores finais são informados de quaisquer vulnerabilidades conhecidas.

G. Controlos que a organização estabeleceu para proteger o hardware (como computadores de secretária, computadores portáteis, dispositivos móveis e outros) contra riscos de cibersegurança, o que inclui a utilização de encriptação, software antivírus, requisitos de palavras-passe complexas, rede privada virtual ou rede de confiança zero para autenticação, atualização periódica do firmware e um processo de gestão de activos que garanta que o hardware emitido pela empresa tem uma configuração de segurança adequada aquando da emissão e eliminação apropriada quando os activos são retirados.

H. Controlos que a organização implementou para garantir que o suporte à produção oferece proteção contra riscos de cibersegurança, o que deve incluir que os servidores sejam corrigidos com versões de segurança em tempo útil para mitigar riscos emergentes. Reveja os controlos de monitorização em vigor para determinar se a disponibilidade e a utilização de recursos estão a ter um desempenho adequado, permitindo que potenciais problemas de cibersegurança que ameacem o desempenho sejam revistos e analisados. Rever os controlos relacionados com as bases de dados, que incluem a limitação do acesso de utilizadores e administradores, a garantia da utilização de encriptação, a cópia de segurança e o teste das bases de dados, bem como a presença de fortes controlos de segurança da rede.

I. Controlos relacionados com a rede que permitem a segmentação para limitar os riscos de cibersegurança decorrentes do acesso não autorizado. Analise a forma como a organização utiliza firewalls, incluindo a localização das firewalls e o processo utilizado para rever, analisar e restringir o acesso à rede, evitando o acesso não autorizado. Analise a forma como a organização utiliza sistemas de deteção/prevenção de intrusão para prevenir, detetar e recuperar de ataques de cibersegurança.

J. Os controlos que a organização estabeleceu em torno dos serviços comuns de comunicação no ambiente de trabalho, como a utilização de encriptação do correio eletrónico, a garantia de que as actualizações de segurança do navegador da Internet são aplicadas atempadamente, as definições de segurança das videoconferências/mensagens (por exemplo, MS Teams, Zoom e outros) estão configuradas para restringir a utilização de determinadas extensões de ficheiros (como ficheiros .exe) e a utilização de autenticação multifactor para a partilha de ficheiros.

K. Controlos que a organização implementou para mitigar os riscos de cibersegurança relacionados com a prestação de serviços, incluindo
    1. Garantir que o processo de gestão de alterações inclui a consideração dos riscos de cibersegurança ao avaliar e aprovar alterações e a resposta atempada a incidentes cibernéticos.
    2. O serviço de apoio ao utilizador regista todos os eventos de cibersegurança comunicados pela organização, assegura a sua resolução atempada e encaminha-os para o membro da administração adequado.
    3. A administração de dispositivos móveis (como correio eletrónico, aplicações e outros) está configurada para reduzir os riscos de cibersegurança e pode ser gerida remotamente se o dispositivo de um utilizador for comprometido.

L. Controlos de segurança física para proteger as informações de alto risco, incluindo os riscos de cibersegurança. Os exemplos incluem a garantia de que o acesso de terceiros/fornecedores é adequado e a limitação do acesso físico dos utilizadores aos centros de dados, centros de operações de rede e centros de operações de segurança ao pessoal autorizado.

M. Controlos que a organização implementou relativamente à resposta e recuperação de incidentes, que devem incluir:
    1. Um plano documentado que é revisto e atualizado à medida que as operações da organização mudam ao longo do tempo.
    2. Testes periódicos e comunicação dos resultados à direção.
    3. Determinar se os problemas identificados pelos testes são resolvidos atempadamente.

Apêndice B. Ferramenta para documentar a conformidade com o requisito temático

Cibersegurança - Governação

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
A. As políticas e os procedimentos relacionados com os processos de gestão dos riscos de cibersegurança são estabelecidos e periodicamente actualizados, incluindo a promoção de práticas baseadas em quadros amplamente adoptados (NIST, COBIT e outros) que reforçam o ambiente de controlo.		
B. As funções e responsabilidades que apoiam os objectivos de cibersegurança da organização estão claramente definidas e as funções estão devidamente preenchidas.		
C. As actualizações dos objectivos, estratégias, riscos e controlos de atenuação da cibersegurança são periodicamente comunicadas ao conselho de administração.		
D. As partes interessadas relevantes são envolvidas no debate sobre a melhor forma de estabelecer e melhorar os processos de gestão dos riscos de cibersegurança.		
E. Os recursos necessários (liderança, financiamento, talento, hardware, software, formação e outros) para executar eficazmente os processos de gestão do risco de cibersegurança são comunicados ao conselho de administração.		

Cibersegurança - Gestão do risco

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
A. Estabelecimento de um processo de gestão do risco a nível da organização que inclua a identificação, análise e gestão dos riscos relacionados com as tecnologias e a segurança da informação, com especial incidência nos riscos de cibersegurança e na forma como esses riscos podem afetar a capacidade da organização para atingir os seus objectivos.		
B. Os processos de gestão do risco de cibersegurança são conduzidos por uma equipa multifuncional que inclui a liderança das tecnologias da informação, a gestão do risco a nível da organização, a gestão jurídica, a gestão da conformidade e outras (por exemplo, operações, contabilidade/finanças) e		

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
envolve partes externas (vendedores, fornecedores, clientes e outros), conforme aplicável.		
C. Foram estabelecidas e são periodicamente actualizadas políticas e procedimentos relacionados com a gestão do risco de cibersegurança, incluindo a promoção de práticas que reforçam os processos de gestão do risco de cibersegurança com base em quadros de gestão do risco amplamente adoptados, orientações oficiais ou melhores práticas.		
D. A responsabilidade pela gestão dos riscos de cibersegurança é estabelecida e foi identificado um indivíduo ou uma equipa que monitoriza e comunica periodicamente a forma como os riscos de cibersegurança estão a ser geridos, incluindo os requisitos de recursos para atenuar os riscos e a identificação de riscos emergentes de cibersegurança que não tenham sido previamente identificados.		
E. É estabelecido um processo para escalar rapidamente os riscos de cibersegurança (emergentes ou previamente identificados) que atingem níveis inaceitáveis com base nas directrizes de gestão de riscos estabelecidas pela organização ou para cumprir os requisitos legais e/ou regulamentares aplicáveis.		
F. A gestão do risco de cibersegurança inclui a coordenação entre a segurança da informação, o departamento jurídico, a conformidade e outros órgãos de gestão para identificar e cumprir todas as obrigações legais e contratuais (leis, regulamentos). O estado de conformidade e não conformidade com os requisitos aplicáveis é comunicado periodicamente à organização.		
G. Está em vigor um processo para identificar e gerir os riscos de cibersegurança relacionados com terceiros. Os vendedores, fornecedores e outros prestadores de processos e/ou serviços subcontratados são contratualmente obrigados a implementar controlos eficazes de cibersegurança que protejam adequadamente a confidencialidade, integridade e disponibilidade dos sistemas e dados da organização a que têm acesso.		
H. As políticas e os processos relacionados com a classificação, retenção, destruição e cifragem dos dados são adequadamente		

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
concebidos e eficazmente aplicados para proporcionar uma abordagem sistemática que garanta o registo completo e exato dos dados e proteja a confidencialidade e a privacidade das informações sensíveis.		
I. Está em vigor um processo de comunicação dos riscos operacionais de cibersegurança para garantir uma sensibilização adequada da direção e dos trabalhadores. As questões, lacunas, deficiências e falhas de controlo são comunicadas ao conselho de administração e à direção e o estado da correção é acompanhado de perto e comunicado. Os incumprimentos das políticas de cibersegurança são identificados, investigados, comunicados e corrigidos atempadamente.		

Cibersegurança - Processos de controlo

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
A. Dá prioridade aos controlos de cibersegurança e assegura que o orçamento e os recursos correspondentes (por exemplo, pessoal, software, ferramentas) são atribuídos para maximizar os benefícios esperados.		
B. Garante que os controlos de cibersegurança estão a funcionar de forma a promover a consecução dos objectivos de cibersegurança da organização e a resolução atempada dos problemas que surjam.		
C. Fornece formação suficiente ao pessoal responsável pelas operações de cibersegurança.		
D. Desenvolveu políticas e procedimentos suficientes para gerir todos os aspectos das operações de cibersegurança e controlos conexos.		
E. Assegura que a administração dispõe dos recursos necessários para se manter informada sobre as questões emergentes de cibersegurança decorrentes das novas tecnologias, identificar oportunidades para melhorar as operações e compreender de que forma os esforços em matéria de cibersegurança podem ser melhor utilizados para ter impacto nas metas e objectivos organizacionais mais amplos.		

Requisito	Conformidade (Sim / Não / Parcial)	Provas obtidas ou justificação da exclusão
F. Integra adequadamente a cibersegurança no ciclo de vida de desenvolvimento do sistema para aplicações comerciais, incluindo software e aplicações adquiridas ou desenvolvidas por medida.		
G. Incluiu a cibersegurança na gestão do hardware (computadores portáteis, computadores de secretária, dispositivos móveis).		
H. Implementou controlos eficazes relativamente ao suporte de hardware de produção, tais como a configuração, a aplicação de patches, o apoio à gestão do acesso dos utilizadores e a monitorização da disponibilidade e do desempenho. A organização avaliou a adequação da conceção e a eficácia operacional destes controlos.		
I. Optimiza os controlos relacionados com a rede no que diz respeito à segmentação da rede, utilização e colocação de firewalls, ligações limitadas a redes e/ou sistemas externos e utilização de tecnologias preventivas e de deteção, tais como sistemas de deteção/prevenção de intrusões.		
J. Implementou controlos eficazes em torno dos serviços comuns de comunicação em ambiente de trabalho, tais como correio eletrónico, programas de navegação na Internet, videoconferência, mensagens e protocolos de partilha de ficheiros.		
K. Implementou controlos adequados da prestação de serviços para garantir que as seguintes áreas estão integradas na monitorização da cibersegurança: gestão de alterações, serviço/balcão de apoio e administração de dispositivos do utilizador final.		
L. Implementou controlos de segurança física adequados para proteger de ataques os centros de informação de alto risco (tais como centros de dados, centros de operações de rede e centros de operações de segurança).		
M. Implementou controlos de resposta a incidentes e de recuperação.		

Sobre o Instituto de Auditores Internos

O Institute of Internal Auditors (IIA) é uma associação profissional que serve mais de 245.000 membros globais e concedeu mais de 195.000 certificações de Certified Internal Auditor (CIA) em todo o mundo. Fundado em 1941, o IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para obter mais informações, visite www.theiia.org.

Declaração de exoneração de responsabilidade

O IIA publica este documento para fins informativos e educativos. Este material não pretende dar respostas definitivas a circunstâncias individuais específicas e, como tal, destina-se apenas a ser utilizado como um guia. O IIA recomenda a procura de aconselhamento especializado independente diretamente relacionado com qualquer situação específica. O IIA não aceita qualquer responsabilidade por quem confie exclusivamente neste material.

Direitos de autor

abril de 2024

Sede mundial
Instituto de Auditores Internos
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, EUA
Telefone: +1-407-937-1111
Fax: +1-407-937-1101