#ESPAÇOCIBER

Questionário traduzido da pesquisa internacional de cibersegurança na gestão de ativos

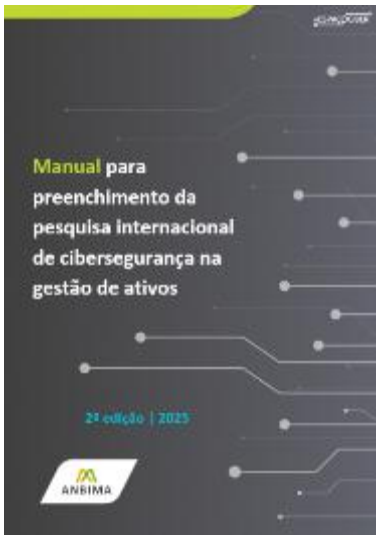
1ª edição | 2025

ANBIMA

Índice

Sobre este material de apoio

Este **Questionário traduzido** é um material de apoio às organizações participantes da Asset Management Cybersecurity Benchmarking Survey (pesquisa de benchmarking de segurança cibernética na gestão de ativos). Organizada pelo Comitê Consultivo dos Membros Afiliados (AMCC, na sigla em inglês) da International Organization of Securities Commissions (Iosco)[1] em parceria com o Investment Company Institute (ICI)[2] desde 2015, a pesquisa é aplicada em diversos países (exceto os Estados Unidos, que conta com pesquisa apartada), inclusive o Brasil.



A ANBIMA, como membro do AMCC-Iosco, atua na disseminação da pesquisa às organizações brasileiras desde a primeira edição, orientando as participantes e acompanhando os envios. Como parte desse esforço, foi elaborado um **Manual**[3] (acesse clicando aqui) para contribuir para o entendimento do funcionamento da pesquisa, a preparação para o preenchimento do questionário, o envio adequado das respostas e o melhor aproveitamento dos resultados.

A versão traduzida do questionário da pesquisa contida neste documento é mais um recurso à disposição das organizações participantes da pesquisa para o preenchimento do questionário final na ferramenta disponibilizada pelo ICI. Este material de apoio contém a localização de termos e pode ser consultado durante o preenchimento do questionário da pesquisa pela(s) pessoa(s) responsável(eis) por esta atividade.

O questionário da edição atual da pesquisa conta com 161 perguntas dispostas em 18 seções, cobrindo uma abrangente variedade de tópicos, visando fornecer uma compreensão completa do estado de maturidade em segurança cibernética das organizações participantes.

A Associação convida as gestoras brasileiras a seguirem participando desta iniciativa anualmente e contribuindo para sua evolução, sublinhando, como elementos fundamentais para a resiliência cibernética dos mercados financeiro e de capitais, a cooperação e o aproveitamento das informações disponíveis para o desenvolvimento das políticas e práticas internas. Como também a se aprofundarem nos tópicos relacionados a este tema no #EspaçoCiber ANBIMA.

[1] Iosco: https://www.iosco.org/.
[2] ICI: https://www.ici.org/.
[3] ANBIMA. Manual para preenchimento da pesquisa internacional de cibersegurança na gestão de ativos (2025). Disponível em: <https://www.anbima.com.br/data/files/76/B2/C1/F4/8FEEA910450F0EA9F82BA2A8/2025_Manual_Pesquisa_Ciberseguranca_IOSCO.pdf>

Questionário traduzido

Seção 1: Perfil da empresa

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
1	Nome da empresa	Nome da empresa	Caixa de texto
2	Insira seu endereço de e-mail	Endereço de e-mail	Caixa de texto
3	Insira seu nome completo.	Nome e sobrenome	Caixa de texto NOME Caixa de texto SOBRENOME
4	Indique o nome da organização e/ou o endereço de e-mail do remetente que encaminhou esta pesquisa para você.	Nome da organização e/ou Endereço de e-mail do remetente da pesquisa	Caixa de texto NOME DA ORGANIZAÇÃO Caixa de texto ENDEREÇO DE E-MAIL DO REMETENTE
5	Número de colaboradores	1 a 10 11 a 50 51 a 100 101 a 500 501 a 1000 1001 a 2000 2001 a 5000 5000 ou mais	Múltipla escolha
6	Selecione todas as regiões onde você tem escritórios.	América do Norte Europa Ásia-Pacífico Oriente Médio e África América Latina e Caribe	Múltipla escolha
7	Você tem escritórios em locais que exigem avaliações de risco e/ou controles de segurança adicionais?	Sim Não	Múltipla escolha
8	Se você tem escritórios em locais que exigem avaliações de risco e/ou controles de segurança adicionais, quais são eles? Selecione todas as opções aplicáveis.	Funcionalidade limitada para usuários Segurança física aprimorada Uso de hardware "local" Restrição do uso de dispositivos corporativos Aplicação de controles de segurança locais Restrições sobre armazenamento de dados locais Monitoramento aprimorado Restrições à transferência transfronteiriça de dados	Múltipla escolha
9	Onde sua empresa implementa sua infraestrutura de TI? Selecione todas as opções aplicáveis.	Data center(s) empresariais Data center(s) de colocation Data center(s) de serviços gerenciados Data center(s) de Nuvem/Infraestrutura como Serviço (IaaS) Não usa data centers	Múltipla escolha

Seção 2: Estrutura de gestão de segurança

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
10	Qual é o cargo da pessoa responsável pelo programa de segurança da informação na sua empresa? **Observação:** Se sua empresa utiliza um CISO virtual (terceirizado), selecione a pessoa responsável por gerenciar o contrato com o fornecedor.	CISO - Diretor de Segurança da Informação CSO - Diretor de Segurança CIO - Diretor de Tecnologia da Informação CTO - Diretor de Tecnologia VP / Diretor / Gerente de Segurança da Informação VP / Diretor / Gerente de TI CCO - Diretor de Compliance GC - Diretor Jurídico COO - Diretor de Operações	Múltipla escolha
11	Onde essa pessoa se encaixa na hierarquia da organização? **Observação:** Adm = Administração Ger. = Gerente Dir. = Diretor VP = Vice-Presidente VPE = VP Executivo VPS = Vice-Presidente Sênior DG = Diretor Gerente DA = Diretor Associado	Cargo executivo sênior / Vice-presidente executivo (VPE) ou equivalente Administração Sênior / VP Sênior / Diretor Gerente ou equivalente Administração de nível médio / VP / DG / DE / Dir. ou equivalente Administração de Linha / DA / Ger. ou equivalente	Múltipla escolha
12	Qual é o número total de funcionários dedicados em tempo integral ou subcontratados que trabalham na sua organização de segurança da informação?	0 1 a 5 6 a 15 16 a 25 26 a 50 51 ou mais	Múltipla escolha
13	Qual é o número total de funcionários ou subcontratados que desempenham funções de segurança da informação como um subconjunto de suas responsabilidades na sua empresa?	0 1 a 5 6 a 15 16 a 25 26 a 50 51 ou mais	Múltipla escolha
14	Qual porcentagem do número fornecido na sua resposta às suas perguntas anteriores são subcontratados?	<5% 5% a <25% 25% a <50% 50% a <75% 75% a <100% 100%	Múltipla escolha
15	A quem o Diretor de Segurança da Informação (CISO), Diretor de Segurança (CSO) ou equivalente da sua empresa se reporta?	CEO - Diretor Executivo CIO - Diretor de Tecnologia da Informação CTO - Diretor de Tecnologia COO - Diretor de Operações CRO - Diretor de Risco CCO - Diretor de Compliance CAO - Diretor Administrativo GC - Diretor Jurídico	Múltipla escolha
16	Você exige que o pessoal de segurança da informação tenha determinadas certificações?	Sim, para a maioria dos cargos Sim, para cargos selecionados Não, isso é incentivado, mas não obrigatório Não, nem incentivado nem exigido	Múltipla escolha

17	Se você respondeu SIM à pergunta anterior, selecione todas as opções aplicáveis.	Liderança (por ex., CISSP, CISM, CRISC) Geral (por ex., Security+, GSEC) Funcional (por ex., CISA, GCIH) Habilidades especializadas (por ex., CEH, OSCP) Tecnologia (por ex., Cloud CCSP) Específico do setor (por ex., financeiro)	Múltipla escolha
18	Indique todas as funções de TI que você terceiriza (Sim, Não, Parcial) para cada uma.	Desenvolvimento e Manutenção de Aplicações Gestão de Auditoria/Compliance Proteção contra Negação de Serviço Help Desk Resposta a Incidentes Testes de Penetração Treinamento de Conscientização em Segurança Serviços do Centro de Operações de Segurança (SOC) Gestão de Risco de Terceiros Gestão de Vulnerabilidades	Múltipla Escolha com Itens da Grade

Seção 3: Governança e Compliance

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
19	Descreva o nível de maturidade da governança da sua segurança da informação (definições abaixo): **Definições:** 1-Inexistente - Não há alinhamento com nenhuma estrutura de segurança cibernética. Não há governança formal. 2-Inicial/Ad hoc - Práticas informais. Pode fazer uma referência vaga ao NIST CSF, aos controles da ISO ou a outra estrutura, mas não tem estrutura. 3-Reproduzível, mas intuitivo - Alinhamento parcial com as estruturas. Há alguns procedimentos documentados. 4-Processo definido - Estrutura formal de governança. As políticas estão alinhadas com o NIST CSF, ISO/IEC 27001 e/ou a orientação normativa. 5-Gerenciado e mensurável - A governança é integrada às plataformas de GRC. As métricas e os KPIs são monitorados. 6-Otimizado - Melhoria contínua com base em inteligência de ameaças, auditorias e lições aprendidas. A IA/ML pode ser utilizada para melhorar a governança.	Inexistente Inicial/Ad hoc Reproduzível, mas intuitivo Processo definido Gerenciado e mensurável Otimizado	Múltipla escolha
20	Você modelou seu programa com base em uma estrutura de segurança? Selecione todas as opções aplicáveis.	Normas ISO/IEC 27000 COBIT Estrutura de Cibersegurança do NIST NIST 800-53 Orientações do Regulador Financeiro (por ex., FFIEC, FINRA, FCA, ESMA, MAS, HKMA) Centro de Segurança da Internet (CIS) Cyber Risk Institute (CRI)	Múltipla escolha

		Padrão de Boas Práticas para Segurança da Informação Cyber Essentials/Cyber Essentials Plus Nenhuma	
21	Você implementou uma plataforma de Governança, Risco e Compliance (excluindo Excel) para gerenciar e acompanhar riscos e conformidade?	Sim Não Não, mas considerando	Múltipla escolha
22	A que tipos de conselhos e/ou comitês você se apresenta? Selecione todas as opções aplicáveis.	Diretoria Corporativa completa Comitê Executivo Comitê de Auditoria Comitê de Risco Comitê(s) Ad Hoc Conselho do Fundo de Investimento Conselho Consultivo	Múltipla escolha
23	Quais das seguintes informações você prepara para Conselhos de Administração (corporativo completo, fundo de investimento ou conselho consultivo)? Selecione todas as opções aplicáveis.	Auditorias Informações de referência Resultados dos testes resumidos de continuidade de negócios Informações sobre o resumo do incidente Indicadores-chave de risco, métricas e progresso Avaliações de risco Estratégia de segurança Informações resumidas sobre o teste de due diligence do fornecedor Informações resumidas sobre o teste de vulnerabilidade N/A - Não fornece informações de cibersegurança a um conselho.	Múltipla escolha
24	Qual é a frequência das apresentações para o conselho corporativo (presenciais ou virtuais)?	Mensal Trimestral Semestral Anual Menos de uma vez por ano (menos frequente do que uma vez por ano) Nunca	Múltipla escolha
25	Você fornece relatórios por escrito além de, ou em vez de, apresentações para o conselho corporativo?	Sim Não	Múltipla escolha
26	Qual é a frequência das apresentações para o conselho corporativo (presenciais ou virtuais)?	Mensal Trimestral Semestral Anual Menos de uma vez por ano (menos frequente do que uma vez por ano) Nunca	Múltipla escolha
27	Você fornece relatórios escritos além de, ou em vez de, apresentações para o conselho do fundo?	Sim Não	Múltipla escolha

Seção 4: Políticas e procedimentos

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
28	Você utiliza serviços de "verificação de identidade" de terceiros (ou seja, verificação de identidade governamental, biometria) para ajudar na avaliação da identidade de subcontratados?	Sim Não Não, mas considerando	Múltipla escolha
29	Você criptografa dispositivos móveis ou dentro de solicitações em dispositivos móveis?	Sim Sim, mas apenas em laptops. Não Não, mas considerando	Múltipla escolha
30	Você realiza revisões de acesso periódicas? Selecione todas as opções aplicáveis.	Contas baseadas em identidades Contas de serviço/genéricas Contas privilegiadas (por exemplo, admin) Conteúdo das funções Associação a funções Nenhuma revisão de acesso realizada	Múltipla escolha
31	Qual é a frequência do seu treinamento de conscientização para todos os usuários? Selecione todas as opções aplicáveis.	Mensal Trimestral Semestral Anual Menos de uma vez por ano Apenas integração (onboarding) Nunca	Múltipla escolha
32	Com que frequência você realiza exercícios simulados de phishing?	Mensal Trimestral Semestral Anual Menos de uma vez por ano (menos frequente do que uma vez por ano) Nunca	Múltipla escolha
33	Se você realizar exercícios simulados de phishing, o que acontece se um usuário falhar? Selecione todas as opções aplicáveis.	Treinamento corretivo imediato Treinamento complementar Notificação do gerente Carta ao funcionário Remoção do cargo Possível demissão Nenhuma ação tomada	Múltipla escolha
34	Se você realizar exercícios simulados de phishing, qual é o limite para ação?	Uma falha Falha em 25% dos testes Falha em 50% dos testes Falha em 75% dos testes Múltiplas falhas conforme determinado pela sua organização.	Múltipla escolha
35	Você exige que todos os funcionários assinem ou reconheçam uma afirmação anual (por exemplo, Política de Uso Aceitável, Segurança da Informação e/ou Política de Proteção de Dados) de	Sim Sim, mas não assinada/reconhecida anualmente. Não Não, mas estou considerando	Múltipla escolha

	que entendem suas responsabilidades em relação à segurança da informação?		
36	Você tem uma política de Traga Seu Próprio Dispositivo (BYOD) que permite o uso de dispositivos pessoais para fins comerciais?	Sim Não Não, mas estou considerando	Múltipla escolha
37	Se você tem uma política de Traga Seu Próprio Dispositivo (BYOD), quais controles técnicos você implementa? Selecione todas as opções aplicáveis.	Os dispositivos são restritos a celulares. Os dispositivos são gerenciados com Gerenciamento de Dispositivos Móveis (MDM) Os dispositivos estão criptografados. As solicitações são gerenciadas pelo MDM ou Gerenciamento de Aplicações Móveis (MAM) Aplicações de comunicação fora do canal estão bloqueados. A conexão com os ativos corporativos é feita por meio de infraestrutura de desktops virtuais (VDI). A conexão aos ativos corporativos é feita por meio de uma rede privada virtual (VPN). Nenhuma das opções acima	Múltipla escolha
38	Você exige que usuários com acesso privilegiado participem de treinamento adicional em cibersegurança (ou seja, além do treinamento de integração)?	Sim Não Não, mas estou considerando	Múltipla escolha

Seção 5: Gerenciamento de riscos

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
39	Com que frequência você realiza avaliações de risco periódicas que revisam ameaças e vulnerabilidades para avaliar sua postura de risco e potenciais consequências adversas para os negócios?	Mensal Trimestral Semestral Anual Menos de uma vez por ano (menos frequente do que uma vez por ano) Nunca	Múltipla escolha
40	Se você realiza avaliações de risco periódicas, quem as completa?	Equipe de Segurança da Informação (ou equivalente) Auditoria Interna Outros internos Gestão de Riscos (Risco de Terceiros / Risco de TI) Provedor de serviço terceirizado	Múltipla escolha
41	Você tem seguro cibernético?	Sim Não Não, mas estou considerando	Múltipla escolha
42	Se você tem seguro cibernético, qual é o valor aproximado da cobertura?	Menos de US$ 5 milhões US$ 5,01 a 10 milhões US$ 10,01 a 20 milhões US$ 20,01 a 50 milhões US$ 50,01 a 100 milhões Mais de US$ 100 milhões	Múltipla escolha

43	Você precisa de avaliações de risco de cibersegurança ou revisões de fornecedores, vendedores ou prestadores de serviços terceirizados?	Sim Sim, mas apenas para terceiros identificados como críticos. Não Não, mas estou considerando	Múltipla escolha
44	Com que frequência você realiza revisões de cibersegurança para seus provedores terceirizados mais críticos?	Monitoramento contínuo e revisões semestrais Monitoramento contínuo e revisões anuais Monitoramento periódico e revisões anuais Monitoramento periódico e/ou revisões ad-hoc (conforme necessário) N/A - Não revisar	Múltipla escolha
45	Quem lidera o processo de revisão de cibersegurança de terceiros?	Segurança da Informação (ou equivalente) Compliance Compras / Financeiro Outros internos Gestão de Riscos (Risco de Terceiros / Risco de TI) Provedor de serviço terceirizado N/A - Não revisar	Múltipla escolha
46	O processo de revisão de terceiros inclui a revisão dos requisitos contratuais para estabelecer controles de segurança e SLAs, incluindo o tempo de notificação de violação?	Sim para todos os fornecedores Sim para fornecedores de maior risco. Não N/A - Não revisar	Múltipla escolha
47	Você utiliza alguma dessas ferramentas e/ou técnicas para monitorar terceiros críticos? Selecione todas as opções aplicáveis.	Ferramentas de terceiros (por exemplo, SecurityScorecard, Bitsight, RiskRecon) Reuniões regulares Relatório regular de métricas Monitoramento automatizado Questionários de segurança anuais Evidências de certificações (por ex., SOC 2) Pesquisas na dark web Nenhuma	Múltipla escolha
48	Você tem um programa formal de riscos/ameaças internas?	Sim Não Não, mas estou considerando	Múltipla escolha
49	Se você tem um Programa Formal de Riscos/Ameaças Internas, qual é o escopo? Selecione todas as opções aplicáveis.	Perda de dados Fraude Sabotagem Facilitação de acesso externo não autorizado à sua rede Violência Violação de políticas acidentais/por negligência	Múltipla escolha
50	Quais desses métodos você utiliza para realizar a verificação de identidades como parte do processo de contratação de novos colaboradores? Selecione todas as opções aplicáveis.	Verificação de documentos (por ex., documento de identidade emitido pelo governo) Verificação biométrica Verificação de bancos de dados (por exemplo, banco de dados oficial) Verificação presencial Verificações de antecedentes Serviços de terceiros Conscientização sobre reconhecimento de deepfake Nenhum	Múltipla escolha
51	Você realiza verificações de antecedentes periódicas em funcionários?	Sim para todos os colaboradores Sim para todos os subcontratados. Sim para todos os colaboradores e subcontratados. Sim, mas apenas para populações de alto risco. Não	Múltipla escolha

52	Se você realiza verificações de antecedentes periódicas em serviço do pessoal, com que frequência elas são concluídas?	Anual Semestral Sob demanda / Conforme necessário	Múltipla escolha
53	Se você realizar verificações de antecedentes apenas para populações de alto risco, quais subpopulações? Selecione todas as opções aplicáveis.	Altos executivos / Executivos seniores Pessoal de TI com acesso privilegiado (por ex., Administradores de Sistema, Help Desk) Gerentes de portfólios Analistas de Investimentos Traders Equipes de Finanças e Operações (pessoal autorizado a gerenciar pagamentos ou liquidações) Pessoal de Atendimento ao Cliente (por ex., Consultores de Investimentos, Gestores de Patrimônio)	Múltipla escolha

Seção 6: Avaliação e Testes de Controle de Segurança

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
54	Você realiza Avaliações de Controle de Segurança (SCA) periódicas para verificar a conformidade com os padrões [por ex., Organização Internacional de Normalização (ISO), National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Center for Internet Security (CIS)]?	Sim Não Não, mas estou considerando	Múltipla escolha
55	Se você respondeu SIM à pergunta anterior, quem realiza as Avaliações de Controle de Segurança (SCA)? Selecione todas as opções aplicáveis.	Segurança da Informação (ou equivalente) Auditoria Interna Outros internos Gestão de Riscos (Risco de Terceiros / Risco de TI) Provedor de serviço terceirizado N/A - Não revisar	Múltipla escolha

Seção 7: Uso de IA e controles de segurança

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
56	Que medidas você está tomando em relação às ferramentas de IA?	Bloqueando toda a IA Habilitando ferramentas de IA aprovadas Nenhuma restrição Nenhuma restrição, monitorado de perto	Múltipla escolha
57	Você tem o seguinte sobre o uso de IA? Selecione todas as opções aplicáveis.	Política de IA Padrão de IA Processos e procedimentos de IA	Múltipla escolha

		Nenhum Nada, mas considerando	
58	Em quais das seguintes áreas a sua empresa está utilizando ou buscando ativamente ferramentas baseadas em IA? Selecione todas as opções aplicáveis.	Atendimento ao Cliente e Marketing (por ex., experiência do cliente aprimorada, resposta a RFPs) Compliance (por ex., análise de vigilância de comunicação, análise regulatória) Segurança da Informação (por ex., análise de logs) Análise de investimentos (por ex., análise de sentimento, resumo de documentos) Jurídico (por ex., revisão de contratos e análise jurídica) Melhorias na produtividade (por ex., automação do fluxo de trabalho, aceleração do desenvolvimento de código) Gestão de Riscos (por ex., análise de riscos e detecção de fraudes) Processos de investimento (por ex., usar a IA para identificar oportunidades de investimento)	Múltipla escolha
59	Onde a governança e supervisão da IA estão na sua empresa? Selecione todas as opções aplicáveis.	A governança / supervisão de IA não está formalizada. Grupo de governança / Supervisão de IA personalizada Segurança de informações Jurídico / Compliance Linhas de negócio Tecnologia Gestão de riscos	Múltipla escolha
60	Você disponibiliza ferramentas de produtividade baseada em IA para sua equipe?	Não Sim, solicitação personalizada fornecida pela empresa. Sim, a empresa implementou ferramentas de IA com controles empresariais e contenção de dados.	Múltipla escolha com Outros
61	Que outras ferramentas de produtividade impulsionadas por IA você disponibiliza para sua equipe? Descreva.	Campo de texto	Campo de texto
62	Você bloqueia ativamente ferramentas de IA não aprovadas?	Sim Sim, utilizando controles do navegador. Sim, utilizando controle da API. Não Não, mas estou considerando	Múltipla escolha

Seção 8: Uso e segurança na nuvem

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
63	Número Total de Provedores de Infraestrutura como Serviço (IaaS) (por ex., Amazon Web Services (AWS), Azure, Google Cloud). Não inclui solicitações de Software como Serviço (SaaS).	0 1 2 3 > 3	Múltipla escolha
64	Sua empresa permite o uso pessoal de solicitações de compartilhamento de	Sim Sim, para certas funções. Não Não, mas estou considerando	Múltipla escolha

	arquivos baseadas na nuvem?		
65	Você utiliza tecnologia para impor políticas de segurança, requisitos de conformidade e proteção contra ameaças para Software como Serviço (SaaS)?	Sim Não Não, mas estou considerando	Múltipla escolha
66	Você realiza varreduras regulares de vulnerabilidades na Infraestrutura como Serviço (IaaS) e na Plataforma como Serviço (PaaS)?	Sim Não Não, mas estou considerando	Múltipla escolha
67	Você realiza testes de penetração regulares na Infraestrutura como Serviço (IaaS) ou Plataforma como Serviço (PaaS)?	Sim Não Não, mas estou considerando	Múltipla escolha
68	Você utiliza infraestrutura em nuvem, gerenciada por você ou por um provedor de serviços, para apoiar seu plano de Continuidade de Negócios/Recuperação de Desastres? Selecione todas as opções aplicáveis.	Sim Sim, para replicação de backup. Sim, para provisionamento rápido de recursos. Sim, para redundância Sim, para distribuição geográfica. Não Não, mas estou considerando	Múltipla escolha

Seção 9: Treinamento de segurança no desenvolvimento de software

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
69	Você mantém um ambiente para testes e desenvolvimento de software e solicitações que é separado do seu ambiente de produção?	Sim Não Não, mas estou considerando	Múltipla escolha
70	Você utiliza o seguinte para gerenciar os riscos de segurança da solicitação? Selecione todas as opções aplicáveis.	Modelagem de ameaças / Análise de segurança Teste de segurança de aplicação estática Teste dinâmico de segurança de aplicações Teste de penetração manual Treinamento de segurança de solicitações Análise de composição de software (software de código aberto)	Múltipla escolha
71	Se você adotou práticas de DevOps, qual é o nível de maturidade do seu programa DevSecOps? (definições abaixo): **Definições:** 1-Inexistente - A segurança não é considerada no ciclo de vida de desenvolvimento de software (SDLC).	Inexistente Inicial/Ad Hoc Reproduzível, mas intuitivo Processo definido Gerenciado e mensurável Otimizado	Múltipla escolha

	Sem alinhamento com quaisquer estruturas de segurança. 2-Inicial/Ad hoc - As práticas de segurança são informais e inconsistentes. As equipes podem implementar medidas básicas de segurança, como varredura de código esporádica ou testes gerais de vulnerabilidade, mas não há uma abordagem estruturada ou padronizada entre os projetos. 3-Reproduzível, mas intuitivo - Integração parcial de segurança no SDLC. Há alguns procedimentos de segurança documentados, e ferramentas básicas de segurança podem ser utilizadas, mas o processo é manual e depende fortemente do conhecimento individual em vez de uma estrutura formalizada. 4-Processo definido - Políticas e procedimentos estão alinhados com estruturas estabelecidas [por ex., NIST Secure Software Development Framework (SSDF)] ou outras orientações regulatórias, garantindo a aplicação consistente de controles de segurança. 5-Gerenciado e mensurável - As práticas de DevSecOps estão integradas com o monitoramento de desempenho. Métricas-chave e KPIs são monitorados para avaliar a eficácia. A governança está integrada com plataformas de GRC para supervisão. 6-Otimizado - Melhoria contínua do programa DevSecOps com base em ciclos de feedback automatizados, inteligência sobre ameaças, auditorias de segurança e lições aprendidas. Tecnologias avançadas como IA/ML são integradas para identificar e mitigar proativamente riscos de segurança.		
72	Você realizou uma avaliação de terceiros dos seus processos de desenvolvimento de software seguro? [por ex., Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM), NIST Secure Software Development Framework (SSDF)]	Sim Não Não, mas estou considerando	Múltipla escolha

Seção 10: Resposta a Incidentes

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
73	Você realiza exercícios simulados periódicos para preparar sua equipe para responder a um evento ou desastre?	Sim Não Não, mas estou considerando	Múltipla escolha
74	Se você realiza exercícios simulados, com que frequência eles são realizados?	Mensal Trimestral Semestral Anual Duas vezes por ano Ad-hoc	Múltipla escolha
75	Se você realiza exercícios simulados, eles estão em um nível técnico, nível de negócios ou em ambos?	Técnico Negócios Ambos	Múltipla escolha
76	Se você realiza exercícios simulados, você inclui prestadores de serviços nesses exercícios? Selecione todas as opções aplicáveis.	Sim, para provedores que realizam funções de cibersegurança (por ex., Provedor de Serviços Gerenciados) Sim, para prestadores que realizam funções críticas de negócios. Sim, com base no cenário. Não	Múltipla escolha
77	Você tem um Plano de Resposta a Incidentes Cibernéticos que é comunicado, mantido e aprimorado?	Sim Não Não, mas estou considerando	Múltipla escolha
78	Se você respondeu SIM à pergunta anterior, com que frequência seu Plano de Resposta a Incidentes Cibernéticos é revisado?	Trimestral Semestral Anual Revisões Ad Hoc Não tenho certeza	Múltipla escolha

79	Quais fontes de inteligência de ameaças cibernéticas (CTI) você utiliza? Selecione todas as opções aplicáveis.	Inteligência de Código Aberto (OSINT) - Cybersecurity and Infrastructure Security Agency (CISA.gov) - Malware Information Sharing Platform (MISP-Project.org) - Fóruns online, blogs, notícias, redes sociais - SANS Intitute Internet Storm Center (ISC.SANS.edu) Inteligência Comercial Fornecedores de CTI de produtos (plataformas e feeds para equipes internas de CTI) Serviços de CTI de fornecedores (análise humana especializada e serviços gerenciados) Provedores de CTI híbridos (por ex., Recorded Future, Mandiant/Google Cloud, Bitsight) Inteligência comunitária - Serviços Financeiros - Centro de Compartilhamento e Análise de Informações (FS-ISAC.com) - Investment Company Institute (ICI.org) - InfraGard (InfraGardNational.org) nos EUA - National Cyber-Forensics and Training Alliance (NCFTA.net) - Securities Industry and Financial Markets Association (SIFMA.org)	Múltipla escolha
80	Você tem um contato no escritório de crimes cibernéticos da Polícia Nacional ou da Lei de sua jurisdição (por ex., FBI)?	Sim Não	Múltipla escolha
81	Se você tem um contato no escritório de crimes cibernéticos da Polícia Nacional ou da Lei de sua jurisdição (por ex., FBI), como você interagiu? Selecione todas as opções aplicáveis.	Chamada ou reunião introdutória Reuniões agendadas regularmente Comunicação contínua Sessões de conscientização realizadas Envolvido em exercícios de simulação	Múltipla escolha
82	Quais das atividades de resposta a incidentes a seguir você automatiza? Selecione todas as opções aplicáveis.	Triagem/priorização de alertas Bloqueio de endereços IP Documentação e relatórios Coleta de inteligência sobre ameaças cibernéticas Isolamento de dispositivos do usuário Isolamento de servidores Bloqueio de contas de usuário Quarentena ou exclusão de arquivo de malware Reimagem do sistema Correção de vulnerabilidades	Múltipla escolha com Outros

Seção 11: Operações e monitoramento de segurança

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
83	Você utiliza sistemas de detecção de anomalias (por ex., análise comportamental) para detectar atividades internas maliciosas?	Sim, totalmente implementado. Sim, mas não totalmente implementado. Não Não, mas estou considerando	Múltipla escolha
84	Se você respondeu SIM à pergunta anterior, indique todos os casos de uso atualmente implementados. Selecione todas as opções aplicáveis.	Detecção de ameaças internas (ou seja, análise comportamental) Monitoramento de usuários privilegiados Detecção de exfiltração de dados Detecção de intrusão em rede (ou seja, análise de comportamento e tráfego de rede) Detecção de fraudes Monitoramento de solicitações (ou seja, anomalias de segurança em aplicações web) Monitoramento de sistema (ou seja, análise de métricas do sistema) Manutenção Preditiva (ou seja, análise de dados de sensores)	Múltipla escolha
85	Você implementou um Centro de Operações de Segurança (SOC) ou uma equipe semelhante dedicada a detectar e responder a incidentes de segurança cibernética?	Sim Sim, terceirizado. Não Não, mas estou considerando	Múltipla escolha
86	Se você tem um Centro de Operações de Segurança (SOC) ou uma equipe semelhante, quantos funcionários estão na sua equipe de Resposta a Incidentes?	1 a 5 6 a 10 11 a 15 16 a 20 21 a 25 >25	Múltipla escolha
87	Quais são os horários do seu Centro de Operações de Segurança (SOC), Centro de Operações de Cibersegurança (CSOC) ou equipe similar?	24/7/365 (Monitoramento contínuo) Horário Comercial Padrão (por ex., 9:00 - 17:00, de segunda a sexta) Horário de Funcionamento Estendido (por ex., 6:00 - 22:00, de segunda a sexta) Sob demanda/Pagamento por uso (serviços de segurança terceirizados, pague conforme necessário)	Múltipla escolha
88	Você utiliza um provedor de serviços de segurança gerenciados para atividades operacionais do dia a dia?	Sim Sim, terceirização de operações de segurança. Não Não, mas estou considerando	Múltipla escolha
89	Você realiza análise de malware internamente?	Sim Não Não, mas estou considerando	Múltipla escolha
90	Se você respondeu NÃO à pergunta anterior, você usa um terceiro? Você utiliza um terceiro para realizar a análise de malware?	Sim Não Não, mas estou considerando	Múltipla escolha

91	Você utiliza ferramentas de Orquestração, Automação e Resposta de Segurança (SOAR) ou ferramentas similares para automatizar a resposta a incidentes?	Sim Não Não, mas estou considerando	Múltipla escolha
92	Você tem metas internas prescritas no Acordo de Nível de Serviço (SLA) para a correção de vulnerabilidades de segurança?	Sim Não Não, mas estou considerando	Múltipla escolha
93	Se você respondeu SIM à pergunta anterior, qual é a meta interna do Acordo de Nível de Serviço (SLA) para corrigir vulnerabilidades de severidade crítica em sistemas expostos à Internet?	Menos de 24 horas 24 a 48 horas 7 dias 14 dias 30 dias Mais de 30 dias	Múltipla escolha
94	Se você respondeu SIM à pergunta anterior, você permite que a aplicação de patches críticos seja adiada devido a possíveis interrupções ou impactos nas operações comerciais?	Sim Não	Múltipla escolha

Seção 12: Controles de Segurança Técnica – Diversos

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
95	Você precisa de dispositivos para autenticar na rede para acesso?	Sim, apenas para a rede com fio. Sim, apenas para a rede sem fio. Sim para ambos. Não Não, mas estou considerando	Múltipla escolha
96	Sua rede sem fio está segregada da sua rede corporativa com fio?	Sim Sim para a rede de convidados Não Não, mas estou considerando	Múltipla escolha
97	Você controla o acesso a sites externos usando controles baseados em rede (por ex., servidores proxy)?	Sim Não Não, mas estou considerando	Múltipla escolha
98	Se você respondeu SIM à pergunta anterior, como você controla o acesso? Selecione todas as opções aplicáveis.	Lista de permissões baseada em categorias Lista de bloqueio baseada em categorias Lista de sites permitidos Lista de sites proibidos Uma combinação de lista de permissões e lista de bloqueios.	Múltipla escolha
99	Você usa um proxy para descriptografar o tráfego e permitir a vistoria de segurança?	Sim Sim, mas resulta em exceções. Não Não, mas estou considerando	Múltipla escolha
100	Você mantém um inventário de todo o hardware, software	Sim, usando ferramentas (por ex., CMDB) Sim, em planilhas ou outros processos manuais.	Múltipla escolha

	e serviços (por ex., Infraestrutura como Serviço (IaaS), Software como Serviço (SaaS))?	Não Não, mas estou considerando	
101	Você proíbe o acesso a e-mails pessoais (por ex., Gmail, Yahoo!)?	Sim Sim, mas apenas para alguns funcionários. Não Não, mas estou considerando	Múltipla escolha
102	Você utiliza backups isolados e/ou imutáveis de sistemas empresariais essenciais?	Sim para isolado. Sim para imutável Sim para ambos. Não Não, mas estou considerando	Múltipla escolha
103	Você usa uma solução de navegador empresarial segura?	Sim Não Não, mas estou considerando	Múltipla escolha

Seção 13: Controles de Segurança Técnica – Viagem

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
104	Você exige que a equipe leve um "dispositivo de viagem" especificamente configurado ao viajar internacionalmente?	Sim para todas as jurisdições / países Sim, mas apenas para jurisdições / países específicos (conforme definido pela sua empresa). Não Não, mas estou considerando	Múltipla escolha
105	Se SIM para a pergunta anterior, este dispositivo é escaneado em busca de ameaças ao ser devolvido?	Sim Não Nenhum dispositivo é reconstruído.	Múltipla escolha
106	Vocês permitem que viajantes internacionais se conectem de volta aos recursos corporativos?	Sim, ao viajar em todas as jurisdições / países. Sim, mas não ao viajar em jurisdições / países específicos (conforme definido pela sua empresa). Não	Múltipla escolha
107	Se a resposta for SIM à pergunta anterior, como os viajantes internacionais se conectam? Selecione todas as opções que se aplicam.	VPN VDI (por ex., Citrix) Serviços de Acesso à Rede com Zero Trust Compartilhamento de arquivos online (por ex., OneDrive) Acesso containerizado a e-mail e calendário (ou seja, controlado por MDM) Outros serviços com controle MDM Limitações determinadas pela jurisdição	Múltipla escolha com Outros
108	Você oferece algum tipo de treinamento antes de viagens internacionais?	Sim, todas as viagens internacionais. Sim, apenas em jurisdições / países específicos (conforme definido pela sua empresa). Não	Múltipla escolha
109	Se você aplicar configurações ou limitações com base na jurisdição, por favor, indique quais jurisdições ou indique N/A para não aplicável.		Texto em Formato Livre
110	Como você decide sobre o risco para os colaboradores e	Revisão da lista de sanções da OFAC Atividade atual da rede de inteligência de ameaças	Múltipla escolha com Outros

	dados em outras jurisdições? Selecione todas as opções aplicáveis.	Avisos de Viagem do Departamento de Estado / Ministério das Relações Exteriores Provedores de Inteligência de Segurança de Viagem (por ex., Kroll, International SOS)	

Seção 14: Controles de Segurança Técnica – Trabalho de Casa (WFH)

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
111	Quais métodos de autenticação baseados em risco fazem parte do seu processo de autenticação para acessar remotamente os sistemas corporativos? Selecione todas as opções aplicáveis.	Senhas Autenticação Multifator (MFA) Verificação de geolocalização Autenticação/confiabilidade do dispositivo	Múltipla escolha
112	Como você está habilitando o acesso remoto para trabalho em casa (WFH/Híbrido)? Selecione todas as opções aplicáveis.	VPN Escritórios Remotos Tecnologias de acesso remoto, por ex., MS RDP, Citrix Acesso direto a recursos baseados na web Não permitimos mais o trabalho remoto.	Múltipla escolha
113	Quais dos seguintes controles de segurança você implementa para trabalho em casa (WFH/Híbrido)? Selecione todas as opções aplicáveis.	Escaneamento de vulnerabilidades Sistemas operacionais/patches necessários Restrições que impedem a impressão Impressão digital de IP ou dispositivos/listas de permissão N/A - Não permitimos mais trabalho remoto.	Múltipla escolha

Seção 15: Controles de Segurança Técnica – Dispositivos do Usuário

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
114	Você restringe o acesso a mídias removíveis em dispositivos de usuários?	Sim, sem leitura ou escrita. Sim, somente leitura. Sim, com escrita limitada. Sim, com leitura limitada. Não Não, mas estou considerando	Múltipla escolha
115	Você usa firewalls pessoais ou suítes de segurança integradas com capacidades de antivírus e firewall?	Sim Sim, mas apenas em laptops. Não Não, mas estou considerando	Múltipla escolha
116	Você utiliza Detecção / Prevenção de Intrusão em Host em dispositivos de usuários?	Sim Não Não, mas estou considerando	Múltipla escolha

117	Você utiliza uma solução de Detecção e Resposta de Endpoint (EDR) em dispositivos de usuários?	Sim Não Não, mas estou considerando	Múltipla escolha
118	Você gerencia dispositivos ou solicitações por meio de soluções de Gerenciamento de Dispositivos Móveis (MDM) ou Gerenciamento de Aplicativos Móveis (MAM)?	Sim para ambos. Sim para MDM Sim para MAM Não Não, mas estou considerando	Múltipla escolha
119	Você proíbe o acesso a plataformas de mídia social em dispositivos dos usuários para atividades não relacionadas ao trabalho?	Sim Sim, mas apenas para alguns funcionários. Não Não, mas estou considerando	Múltipla escolha
120	Você permite que os usuários finais tenham acesso administrativo em seus desktops/laptops?	Sim Sim, mas apenas em circunstâncias aprovadas. Sim, mas considerando restringir. Não	Múltipla escolha
121	Você exige que a equipe realize funções administrativas a partir de estações de trabalho isoladas, protegidas e monitoradas?	Sim Sim, em situações de risco específicas. Não Não, mas estou considerando	Múltipla escolha

Seção 16: Gerenciamento de identidades e acessos

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
122	Qual é o **mínimo** de caracteres que você exige para senhas de contas não administrativas?	< 8 caracteres 8 - 11 caracteres 12 - 14 caracteres 15 - 16 caracteres > 16 caracteres	Múltipla escolha
123	Qual é o **mínimo** de caracteres que você exige para senhas de contas administrativas/privilegiadas?	< 12 caracteres 12 - 15 caracteres 16 - 20 caracteres 21 - 25 caracteres > 25 caracteres	Múltipla escolha
124	Qual é o **tamanho mínimo** de senha que você exige para contas do sistema/solicitação (contas de serviço)?	< 12 caracteres 12 - 15 caracteres 16 - 20 caracteres 21 - 25 caracteres > 25 caracteres	Múltipla escolha
125	Você implementa filtros de força de senhas para avaliar senhas escolhidas em relação a padrões comuns, dicionários e senhas conhecidas que foram expostas?	Sim Não Não, mas estou considerando	Múltipla escolha

126	Com que frequência sua empresa exige que não-administradores troquem senhas? Selecione todas as opções aplicáveis.	A cada 60 dias A cada 90 dias A cada 120 dias A cada 180 dias A cada 365 dias Quando há evidências de comprometimento do autenticador. Quando uma vulnerabilidade relacionada ao algoritmo de hash de senhas é descoberta Nunca	Múltipla escolha
127	Com que frequência sua empresa exige que os administradores troquem as senhas? Selecione todas as opções aplicáveis.	A cada 30 dias A cada 60 dias A cada 90 dias A cada 120 dias A cada 180 dias Quando há evidências de comprometimento do autenticador. Quando uma vulnerabilidade relacionada ao algoritmo de hash de senhas é descoberta Nunca	Múltipla escolha
128	Você utiliza software de gerenciamento de senhas? (por ex., definição genérica)	Sim Sim, apenas para administradores. Não Não, mas estou considerando	Múltipla escolha
129	Você implementou padrões de senha (por ex., NIST-800-63)?	Sim Sim, exceto por mudar senhas apenas quando comprometidas. Sim, parcialmente/em andamento Não Não, mas estou considerando Não use autenticação sem senha, em vez disso.	Múltipla escolha
130	Você utiliza autenticação biométrica, como reconhecimento facial ou de impressões digitais, para acesso a sistemas corporativos?	Sim Não Não, mas estou considerando	Múltipla escolha
131	Você utiliza autenticação biométrica, como reconhecimento facial ou de impressão digital, para acessar dispositivos móveis?	Sim Não Não, mas estou considerando	Múltipla escolha
132	Se você usar autenticação biométrica (por ex., reconhecimento facial ou de impressões digitais), os usuários são obrigados a "optar por participar" para consentir o uso de biometria?	Sim Não	Múltipla escolha
133	Sua empresa implementa autenticação baseada em risco (ou seja, geolocalização, confiança no dispositivo) como parte de seus processos de autenticação para acessar internamente os sistemas corporativos?	Sim Não Não, mas estou considerando	Múltipla escolha
134	Se você respondeu NÃO ou NÃO, MAS CONSIDERANDO à	Conformidade com regulamentos ou estrutura Preocupações de segurança	Múltipla escolha

	pergunta anterior, qual das opções a seguir teria a maior influência na sua decisão? Selecione todas as opções aplicáveis.	Impacto no usuário Resistência do auditor Impacto do seguro cibernético	
135	Você exige autenticação multifator (MFA) para acesso dentro da rede corporativa?	Sim Sim, mas apenas para alguns acessos. Não Não, mas estou considerando	Múltipla escolha
136	Você exige autenticação multifator (MFA) para acesso administrativo sempre que possível, mesmo ao acessar internamente?	Sim Sim, mas apenas para alguns sistemas. Não Não, mas estou considerando	Múltipla escolha
137	Você precisa de autenticação multifator para elevar privilégios?	Sim Não Não, mas estou considerando	Múltipla escolha
138	Você utiliza um modelo zero-trust para acesso à rede interna?	Sim Não Não, mas estou considerando	Múltipla escolha
139	Você utiliza um modelo zero-trust para acesso remoto à rede?	Sim Não Não, mas estou considerando	Múltipla escolha
140	Você monitora o acesso administrativo no nível de cada tecla pressionada?	Sim Não Não, mas estou considerando	Múltipla escolha

Seção 17: Criptografia

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
141	Seu roteiro de Criptografia Pós-Quântica (PQC) inclui o seguinte? Selecione todas as opções aplicáveis.	Atualizar algoritmos para troca de chaves Mudar a forma como os certificados digitais são emitidos e gerenciados Atualizar gerenciadores de segredos e chaves para lidar com chaves para algoritmos de PQC. Implementar Módulos de Assinatura de Hardware Revisar os roteiros de PQC dos fornecedores Não começamos um roteiro.	Múltipla escolha
142	Você criptografa mídias de backup fora do local?	Sim Não Não ter mídia de backup fora do site.	Múltipla escolha
143	Você criptografa compartilhamentos de arquivos internos?	Sim Somente Sensível Não Não, mas estou considerando	Múltipla escolha
144	Você criptografa bancos de dados internos?	Sim, criptografamos totalmente os bancos de dados internos (por ex., Criptografia de Dados Transparente). Sim, usamos criptografia granular (por ex., em nível de coluna ou em nível de campo). Sim, usamos um método diferente (por ex., no nível do sistema de arquivos ou de hardware) Não, nós não criptografamos nossos bancos de dados internos, mas estamos considerando isso.	Múltipla escolha

145	Você utiliza um provedor de serviços de armazenamento (SSP) ou Armazenamento como Serviço (STaaS)?	Sim Não Não, mas estou considerando	Múltipla escolha
146	Se você respondeu SIM à pergunta anterior, o SSP ou STaaS criptografa seus dados?	Sim Não Não, mas estou considerando	Múltipla escolha
147	Você criptografa dados internos em movimento?	Sim Dados/sistemas sensíveis apenas Não Não, mas estou considerando	Múltipla escolha
148	Você rastreia e remedia protocolos e algoritmos obsoletos ou inseguros, por ex., Secure Socket Layer (SSL) v3, Transport Layer Security (TLS) v1.0/1.1?	Sim Não Não, mas estou considerando	Múltipla escolha
149	Você criptografa TODAS as informações não públicas (NPI) em repouso?	Sim Não Parcial, com controles compensatórios aprovados	Múltipla escolha

Seção 18: Controles de segurança de dados

QUESTÃO	PERGUNTA	OPÇÕES DE RESPOSTA	FORMATO DA RESPOSTA
150	Você oferece autenticação multifator (MFA) para acesso dos clientes aos seus dados?	Sim, é necessário para todo acesso. Sim, está disponível como uma opção. Sim, é necessário para alguns níveis de acesso (por ex., transações). Não Não, mas estou considerando	Múltipla escolha
151	Você utiliza autenticação baseada em risco (ou seja, alteração dos requisitos de autenticação com base no comportamento ou características do cliente) para acesso do cliente?	Sim Não Não, mas estou considerando	Múltipla escolha
152	Você tem uma política de classificação de dados?	Sim Não Não, mas estou considerando	Múltipla escolha
153	Se você tem uma política de classificação de dados, você exige o uso de rótulos de sensibilidade em documentos e/ou áreas de armazenamento de documentos para indicar a classificação?	Sim, com rotulagem manual. Sim, com rotulagem automatizada. Não Não, mas estou considerando	Múltipla escolha
154	Se você tem uma política de classificação de dados, você usa ferramentas para identificar e impor rótulos de classificação e sensibilidade?	- Sim, ferramentas para classificar automaticamente dados estruturados com base no conteúdo. - Sim, ferramentas para classificar automaticamente dados não estruturados com base no conteúdo. - Sim para impor a exigência de aplicar classificação	Múltipla escolha

	Selecione todas as opções aplicáveis.	quando os documentos são criados. - Sim para usar tecnologia de gerenciamento de direitos para aplicar controles de segurança com base nos dados e/ou na classificação de sensibilidade. - Não	
155	Você permite que reuniões sejam gravadas, transcritas e resumidas usando ferramentas de IA?	ITENS DA GRADE: A. Gravações de reuniões B. Transcrições de reuniões C. Resumos das reuniões OPÇÕES DE RESPOSTA: 1. Sim, permitido para todos. 2. Sim, permitido, mas apenas para usuários autorizados. 3. Não, não é permitido	Múltipla Escolha com Itens da Grade
156	Para reuniões gravadas, transcritas ou resumidas por IA, quais controles você implementou? Selecione todas as opções aplicáveis.	Treinamento de colaboradores Ferramentas aprovadas Os usuários devem reconhecer a gravação. Restrito pelo tema da reunião Restrito pelos participantes da reunião Gerenciar o acesso a transcrições Sem controles	Múltipla escolha
157	Você usa anexos de e-mail para comunicar detalhes financeiros para/de seus clientes?	Nenhum cliente da empresa troca arquivos apenas por meio de um portal/solicitação autenticado. Sim, mas apenas para alguns clientes institucionais. Sim, para alguns clientes institucionais e não institucionais.	Múltipla escolha
158	Se você usa anexos de e-mail para comunicar detalhes financeiros com seus clientes, aproximadamente que % dos clientes ainda se comunicam com e-mails contendo anexos de arquivo?	<5% 5% a <25% 25% a <50% 50% a <75% 75% a < ou = 100%	Múltipla escolha
159	Se você usa anexos de e-mail para comunicar detalhes financeiros com seus clientes, qual é a principal razão para não eliminar a comunicação por e-mail com os clientes?	Preferência do cliente Práticas legadas Deficiências no controle de segurança Outras prioridades	Múltipla escolha
160	Quais capacidades de site você oferece aos clientes? Selecione todas as opções aplicáveis.	Relatório Manutenção da conta Transações	Múltipla escolha
161	Você impõe controles sobre impressão em sua empresa? Selecione todas as opções aplicáveis.	A impressão é desativada por padrão. A impressão é habilitada por exceção. A impressão é restrita com base na localização. A impressão de seguir-me está implementada.	Múltipla escolha